Київський національний університет технологій та дизайну

ТЕХНОЛОГІЇ ТА ІНЖИНІРИНГ

Науковий журнал

Том 26, № 4, 2025

Київ
2025

ISSN 2786-5371
e-ISSN 2786-538X

Засновник журналу:
Київський національний університет технологій та дизайну

Рік заснування: 1999 р.

Періодичність випуску: 6 разів на рік

Рекомендовано до друку та поширення
через мережу Інтернет Вченою Радою
Київського національного університету технологій та дизайну
(протокол № 2 від 17 вересня 2025 р.)

Державна реєстрація:
Ідентифікатор медіа: R30-05423
Рішення Національної ради України з питань телебачення і радіомовлення № 2520,
протокол № 22 від 8 серпня 2024 року

Журнал внесено до категорії «Б» Переліку наукових фахових видань України,
відповідно до якого можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора та кандидата наук зі спеціальностей:
технічні (наказ Міністерства освіти і науки України № 735 від 29 червня 2021 р.):
122 – Комп'ютерні науки, 131 – Прикладна механіка, 133 – Галузеве машинобудування, 151 – Автоматизація та комп'ютерно-інтегровані технології, 161 – Хімічні технології та інженерія, 132 – Матеріалознавство, 182 – Технології легкої промисловості, 141 – Електроенергетика, електротехніка та електромеханіка, 144 – Теплоенергетика, 171 – Електроніка.

Журнал представлено у міжнародних наукометричних базах даних, репозитаріях та пошукових системах: Національна бібліотека України імені В. І. Вернадського, Crossref, Google Scholar, Litmaps, OUCI, Фахові видання України, EBSCO, Dimensions, UCSB Library, University of Oslo Library, University of Hull Library, BASE, Ulrichsweb Global Serials Directory

Адреса редакції:
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
тел/факс: +38 (044) 256-84-27
E-mail: knutd@technologies-engineering.com.ua
https://technologies-engineering.com.ua/uk

Kyiv National University of Technologies and Design

TECHNOLOGIES AND ENGINEERING

Scientific Journal

Vol. 26, No. 4, 2025

Kyiv
2025

ISSN 2786-5371
e-ISSN 2786-538X

Founder:
Kyiv National University of Technologies and Design

Year of foundation: 1999

Frequency: 6 issues per year

Recommended for printing and distribution
via the Internet by the Academic Council
of Kyiv National University of Technologies and Design
(Minutes No. 2 September 17, 2025)

State registration:
Media identifier: R30-05423
Decision of the National Council of Television and Radio Broadcasting of Ukraine No. 2520,
Minutes No. 22 dated 08.08.2024

The journal is included in category "B" of the List of scientific professional publications of Ukraine, in which the results of dissertations for the degree of doctor and candidate of sciences can be published in the following specialties: technical (Order of the Ministry of Education and Science of Ukraine No. 735 dated 29.06.2021): 0612 – Database and network design and administration, 0715 – Mechanics and metal trades, 0714 – Electronics and automation, 0711 – Chemical engineering and processes, 0588 – Inter-disciplinary programmes and qualifications involving engineering, manufacturing and construction, 0723 – Textiles (clothes, footwear and leather), 0713 – Electricity and energy, 0714 – Electronics and automation

The journal is presented in the international scientometric databases, repositories and scientific systems: Vernadsky National Library of Ukraine, Crossref, Google Scholar, Litmaps, OUCI, Professional Publications of Ukraine, EBSCO, Dimensions, UCSB Library, University of Oslo Library, University of Hull Library, BASE, Ulrichsweb Global Serials Directory

Editors office address:
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
tel/fax: +38 (044) 256-84-27
E-mail: knutd@technologies-engineering.com.ua
https://technologies-engineering.com.ua/en

Редакційна колегія

Редакційна колегія

Editorial Board

Editorial Board

ЗМІСТ

CONTENTS

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 22.04.2025
Revised: 18.08.2025
Accepted: 17.09.2025

UDC 004.056.5:004.8

DOI: 10.30857/2786-5371.2025.4.1

AI vs AI: Using artificial intelligence to protect data and attacks on it

Igor Rudenko*
Master
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0008-3582-3951

Abstract. The aim of the study was to conduct a comprehensive analysis of the role of artificial intelligence as a tool for attacks and defence in information systems, with a focus on evaluating the effectiveness of existing approaches and justifying prospects for integrating artificial intelligence to enhance cybersecurity under conditions of increasing intelligent threats. Within the framework of the study, the confrontation between offensive and defensive artificial intelligence systems in a dynamic environment with adaptive behaviour was modelled, which made it possible not only to identify typical threat vectors but also to assess the effectiveness of corresponding countermeasures. It was found that generative models, particularly those based on reinforcement learning, effectively adapted to defensive responses, bypassing traditional filters and heuristics. At the same time, the highest resilience to such attacks was demonstrated by combined approaches that integrated Federated Learning, blockchain, and differential privacy: the level of resistance to attacks increased by up to 40% with a moderate decrease in accuracy (3-6%). Adversarial training ensured an increase in security of up to 25%, although the accuracy dropped by up to 4%, and its effectiveness depended significantly on the completeness and variability of training data. Homomorphic encryption proved to be the most confidential approach, but remained limited in practical use due to excessive resource consumption and processing time. Although blockchain tools contributed to transparency and data immutability, these tools involved high latency, which complicated the application in real-time conditions. Overall, the results of the study confirmed the appropriateness of using multimodal, adaptive, and multi-level protection strategies for artificial intelligence systems, especially amid the growing number of generative attacks, as evidenced by real cases (e.g., Disney). The practical significance lay in the formation of foundations for the development of adaptive cyber defence systems capable of countering intelligent attacks in real time. The obtained results could be used to enhance the security of critical infrastructure, financial platforms, and autonomous systems

Keywords: data privacy; generative networks; phishing; biometric system; deepfakes

Introduction

The relevance of the study stemmed from the rapid development of artificial intelligence (AI), which played a key role in modern cybersecurity systems. However, alongside this, the use of AI for attacks also increased, significantly complicating traditional methods of information protection. Modern offensive systems, due to the ability to adapt and evolve in real time, could bypass traditional protection methods, change malware signatures, create phishing messages, or attack biometric systems. This created new challenges for cybersecurity professionals and required the development of innovative approaches to designing defensive systems capable of independently adapting to new threats. The "AI vs AI" system had become a reality, where attacks and defence continuously interacted, learning from each other – presenting researchers with the task of creating AI capable of effectively countering hostile intelligent systems. This study considered the effectiveness of such interactions and proposed new strategies for developing defensive systems that could form the foundation for enhancing cybersecurity amid escalating technological threats.

During the period 2020-2025, the topic of "AI vs AI" confrontation attracted the attention of many researchers,

Suggested Citation:
Rudenko, I. (2025). AI vs AI: Using artificial intelligence to protect data and attacks on it. *Technologies and Engineering,* 26(4), 11-25. doi: 10.30857/2786-5371.2025.4.1.

*Corresponding author

who proposed various approaches to building both defensive and offensive systems based on AI. To form a comprehensive view of this issue, the conditional findings of ten authors whose research was considered relevant to the selected topic were analysed. G. Pu *et al.* (2020) focused on developing a hybrid intrusion detection system based on a combination of unsupervised learning and clustering methods. The authors showed that such a system detected new types of attacks but faced the problem of a high number of false positives when the network topology changed. S. Al-Ahmadi *et al.* (2022) investigated the use of Generative Adversarial Network (GAN) for generating phishing emails capable of bypassing modern anti-phishing filters. The results demonstrated the ability of AI-attacks to outperform traditional filtering tools, highlighting the need for new forms of dynamic content analysis. D. Calvaresi *et al.* (2021) proposed the use of reinforcement learning agents for continuous real-time system monitoring and demonstrated the effectiveness of this approach under changing input data, but noted that the models required significant training and computational resources. R.R. Gopireddy (2024) analysed data poisoning attacks, where the attacker manipulated training sets to distort the performance of the defensive AI. The results showed that even slight data distortion significantly reduced the accuracy of deep learning-based models.

J. Wu *et al.* (2022) presented a multi-level defence system based on an ensemble of models that intercepted complex multistep attacks. At the same time, the authors pointed out the risks of excessive complexity, which complicated the interpretability of model decisions. D.L. Marino *et al.* (2025) proposed the use of transformer architectures to analyse network traffic for anomaly detection. The approach demonstrated high accuracy but remained vulnerable to attacks that mimicked legitimate user behaviour. A. Ragmani *et al.* (2020) studied the effectiveness of adaptive neural network-based models for protecting cloud services. The research showed that such models coped better than traditional ones with Distributed Denial of Service (DDoS) attacks, but worked less effectively under limited input data. K. Santhi *et al.* (2024) conducted an analysis of ethical risks associated with the use of AI in defensive systems, particularly the likelihood of false user identification or breaches of confidentiality. The authors emphasised the need to ensure algorithmic transparency during implementation. M. Hasan (2024) explored the integration of defensive models with blockchain technologies to counter event log modification in cyberinfrastructure. The solution demonstrated resistance to manipulation but required optimisation for transaction processing delays. P.S. Muhuri *et al.* (2020) developed an attack vector prediction system based on historical data and deep recurrent networks. The approach reduced incident response time by 30%, but proved less effective under conditions of data scarcity or non-representativeness.

Thus, the summarised analysis showed that no approach was universal. The development of the "AI vs AI" direction required not only engineering innovations but also a deep interdisciplinary understanding in the fields of machine learning, ethics, security, and information technology. Despite significant progress in applying AI to protect information systems, a number of important aspects remained insufficiently researched. In particular, most existing approaches focused on the isolated use of AI either for attacks or for defence, whereas the dynamic interaction between offensive and defensive AI systems in real time remained limited in study. Insufficient attention was also paid to the resilience of defensive models in the case of combined intelligent attacks involving multiple tactics – for example, data poisoning alongside phishing or social engineering. Furthermore, the question of defensive systems' adaptability to rapidly evolving threats posed by self-learning attack algorithms remained open. All of this determined the need for a deeper study of the "AI vs AI" confrontation in the context of the dynamic and complex environment of modern cybersecurity.

The aim of the study was to determine the effectiveness and limitations of modern AI-based defence tools in the context of evolutionary confrontation with AI attacks, with the further justification of directions for improving the cyber resilience of information systems. To achieve this aim, the following tasks were set: to model typical interaction scenarios between defensive and offensive AI, identify critical vulnerabilities in defensive model performance under intelligent attacks, and propose approaches to increasing the adaptability and effectiveness of defensive systems in a constantly changing threat environment.

Materials and Methods

This study implemented a multi-level approach to the analysis and modelling of the confrontation between offensive and defensive AI under conditions of escalating cyber threats and increasing complexity of digital infrastructures. The primary objective was to build a conceptual and practical model of interaction between AI systems within the "AI vs AI" scenario, reflecting the realities of modern cyberspace where both sides of the conflict could employ intelligent agents. The study analysed scientific publications, real-world attack cases, and statistical data covering the period from 2020 to March 2025. This timeframe made it possible to trace the evolution of offensive and defensive strategies of AI systems, as well as to monitor changes in the frequency, complexity, and effectiveness of security incidents. The analysis used sources from academic publications, technical documentation, cybersecurity reports, and open cases of digital infrastructure breaches.

Particular attention was paid to generative attacks, especially face falsification using GANs, in the context of the increasing difficulty of detecting forgeries in biometric systems. Physical objects such as glasses with modified textures were considered as potential tools for carrying out subtle attacks on facial recognition systems. In the field of attacks on text-based systems, the use of stylometric analysers and filters focused on detecting AI-generated

phishing messages was analysed. The study also covered novel approaches to model inversion based on facial reconstruction from latent space using diffusion mechanisms. Among the examined countermeasures was the use of federated learning to reduce data compromise risks through decentralised processing. In the cryptographic domain, the application of fully homomorphic encryption was analysed, allowing computations to be performed on encrypted data without decryption. Additionally, in the context of dynamic deployment of security infrastructure, the use of unmanned aerial vehicles as mobile nodes capable of adaptively responding to threats in real time was explored.

The first stage of the study involved developing a classification system for offensive AI agents that enabled a structured representation of the functionality, goals, adaptability, and level of autonomy. The classification considered four key parameters: type of action (analytical, generative, manipulative), training model (static training, continuous learning, reinforcement learning), attack target (data, infrastructure, user), and level of autonomy (human-operated, semi-autonomous, fully autonomous agents). This made it possible to identify the most high-risk combinations of traits – for example, fully autonomous agents with generative functions that adapted to environmental changes in real time. The second stage included practical modelling and simulation of interaction scenarios between AI agents on both sides. Frameworks such as TensorFlow 2.0, PyTorch, and the OpenAI Gym environment were used to implement the models. The agents were implemented as modules with clearly distributed functions: offensive agents generated penetration scenarios, data manipulation, or deception model training, while defensive agents performed detection, classification, blocking, or recovery. Particular attention was paid to adversarial examples, where minimal changes in input data could result in misclassification. The third stage involved a comparative analysis of simulation results. The effectiveness of system interaction was assessed using several criteria: average attack detection time, classification accuracy, false positive rate, model adaptability, and computational costs for both sides. The obtained data made it possible to identify weak points in defence systems under conditions of dynamic offensive strategies. Real-world cases were also used to build simulations. Thus, the research methodology combined theoretical generalisation with practical modelling, providing in-depth understanding of the characteristics of the confrontation between intelligent systems under next-generation cyber threats.

Results

Classification of AI attack tools and defence strategies in a dynamic environment. In the context of the "AI vs AI" confrontation study, it is appropriate to classify AI tools used for attacks according to several criteria: type of action, training method, usage purpose, and level of autonomy. Depending on the type of action, offensive AI was categorised as information-analytical, generative, and aggressively influential. Information-analytical agents were used to collect and process data on the target, identify vulnerabilities, and analyse user behaviour, particularly through the use of natural language processing to scan open sources. Generative models, including GANs, enabled the creation of fake images, videos, messages, and other content used in phishing campaigns or social engineering attacks. Aggressively influential models were aimed at actively disrupting systems – through injecting malicious data into training sets, generating input data to deceive the model, or modifying data during transmission.

By training method, these AI systems were divided into pre-trained and adaptive. The former relied on a pre-formed knowledge base and were designed for mass attacks, while the latter learned in real time, adjusting the behaviour based on the defence system's responses, increasing the attack's effectiveness. According to the usage purpose, attacks targeted data, models, or users. Data attacks involved stealing, encrypting, or destroying information using intelligent analysis of file structures and access rights. Model attacks aimed at reverse engineering or identifying weaknesses in the defence system's logic. In turn, user-targeted attacks involved imitating human behaviour, personalising phishing messages, or manipulative communication based on psychological profiling (Karl & Potter, 2023).

AI-based attacks and defences exist in constant dynamic – offensive AI analyses vulnerabilities in defensive systems, attempts to bypass protective measures, and finds new paths for intrusion, while defensive AI, in turn, adapts to these changes. For instance, when generative models (like GANs) are used to create fake data, a defensive system may detect such data through anomaly pattern analysis, making it increasingly difficult over time for offensive models to succeed. However, defence systems must respond to these changes in time, otherwise an attack may succeed. This battle is often cyclical: attacks evolve, and the discovery of new vulnerabilities or strategies is continuously followed by improved defence models (Kumar *et al.*, 2024). A distinctive feature of the interaction between offensive and defensive AI is the adaptability of both sides. In the modern environment, where offensive systems can actively adjust to new conditions and defence strategies, defensive AI systems must also possess self-learning capabilities. For example, the use of adversarial training enables defence systems to "learn" from attacks, improving resilience. Offensive AI, using methods that adapt to new defence techniques (e.g., developing new attacks based on the analysis of previous results), forces defence to constantly evolve (Shah, 2024). This means that the defence system must quickly react to new attack methods, continuously updating detection models and techniques. Systems that self-learn and use artificial neural networks to analyse large volumes of data can offer high adaptability even to unforeseen types of attacks.

According to the latest studies, the frequency of AI-driven data attacks increased between 2020 and 2025. Specifically, in 2023 the number of phishing attacks rose

by 265% compared to the previous year, many of which were AI-generated. It is projected that by 2025, 45-50% of phishing emails targeting businesses may be generated using AI, with victim response rates rising to 62-65%. Furthermore, in 2024 a rise in AI-based attacks was observed, accounting for approximately 40% of all cyber threats (Martin, 2025). These trends highlighted the need for effective defence strategies against AI-powered attacks. In particular, attention should be paid to multimodal authentication, the use of synthetic data detection algorithms, and the implementation of differential privacy mechanisms. It is also important to restrict open access to model APIs and implement query frequency control to prevent model inversion attacks.

It is critical to note that certain shared vulnerabilities exist across both offensive and defensive systems. These are often linked to data limitations used for training AI models. For example, if the defence system's training dataset is incomplete or inaccurate, the offensive system may find a "breach" by exploiting undocumented vulnerabilities. Conversely, if the offensive system uses adversarial attack methods, its effectiveness may depend on the accuracy and volume of its training data. If these data are insufficiently comprehensive, the offensive system may become vulnerable to countermeasures from the defence side. Therefore, the interaction between offensive and defensive AI systems is complex and multifaceted (Truong *et al.*, 2020). This is a constantly evolving field, where each side's effectiveness depends on the ability to adapt to changing conditions, as well as on real-time self-learning and evolution. In the "AI vs AI" sphere, attacks on information systems using AI take various forms and implementation methods. Some of the most effective approaches include the use of GANs, adversarial input, and reinforcement attack methods. Each of these has distinct features and capabilities for bypassing existing defence systems. GANs are powerful tools for generating fake data or content that can mislead detection systems. A GAN consists of two main components: a generator, which creates new data, and a discriminator, which tries to determine whether the data are fake. These two components operate in a competitive manner: the generator attempts to create data realistic enough to fool the discriminator, while the discriminator tries to distinguish real from generated data (Navidan *et al.*, 2021). In the context of AI attacks, GANs can be used to generate fake images, videos, voice recordings, or texts for social manipulation, phishing, or even manipulation of machine learning outcomes. For instance, GANs can create fake faces so realistic that it is possible to deceive biometric systems.

Adversarial input attacks involve the attacker crafting specially designed inputs that mislead a machine learning model, causing it to make incorrect predictions or decisions. Adversarial inputs are visually imperceptible to humans but can severely disrupt the system's functionality, especially in neural networks that are sensitive to minor input perturbations. This type of attack includes modifying images, text, or other information so that the model misinterprets the data. For example, altering individual pixels on an image may cause a neural network to misclassify it, even though the image appears unchanged to the human eye. This method can be used to bypass security systems based on machine learning, such as facial recognition or suspicious transaction verification systems. Reinforcement attacks use reinforcement learning principles to optimise the attack strategy. In this approach, the offensive agent uses a system of rewards and penalties to build the most effective strategy for evasion. These attacks typically involve interactive learning, where the agent observes the defence system's reactions and adjusts its strategy accordingly. This type of attack is especially dangerous due to its ability to self-optimise. The offensive system learns the defensive AI's behaviour and adapts to its responses, continuously improving its methods to achieve its goal. As a result, reinforcement attacks can effectively bypass even advanced defence algorithms, since the attacking agent can adjust its actions in real time.

Machine learning models used in defence systems can be vulnerable to modification or reconstruction attacks. Model attacks usually aim to gain access to the confidential training data. In particular, hackers may attempt to reconstruct model parameters or even recover data used in training, enabling deception or forgery of the system. Models built on large datasets can be especially vulnerable to this kind of attack, as attackers may exploit partial information about model behaviour to reconstruct internal parameters or training data structure, thereby targeting specific vulnerabilities (He *et al.*, 2020). Context-oriented attacks are another complex method in which the attacking system considers not only the data itself, but also the context in which the data are transmitted. These attacks can target the detection or manipulation of certain aspects of an information system based on the context in which it operates. This allows for more effective attacks, as the system adapts to the specific conditions and vulnerabilities inherent to a given context (Jiang *et al.*, 2022).

Such attacks often leverage a deep understanding of the defence system's internal logic and its responses to certain data types, allowing the attacking agent to tailor its actions to match the conditions of the specific situation in which the attack occurs. Thus, the use of tools such as GANs, adversarial input, and reinforcement attacks enables attackers to bypass security mechanisms efficiently, adapting to changes and improving the strategies in real time. As these methods allow offensive systems to learn and adapt to defences, developing new countermeasures becomes complex but vitally important for ensuring security in the AI era. The integration of AI into cyber threats has created a new class of attacks characterised by adaptability, feedback learning, and high levels of disguise. For defence systems, this means not only increased detection difficulty but also the need for rapid adaptation to environmental changes. Table 1 provided a classification of the main types of AI-based attacks, the descriptions, practical examples, and potential consequences for information security.

***Table 1**. Types of AI attacks and the characteristics*

Type of attacks	Description	Application example	Potential consequences	Attack effectiveness
GAN	Creating fake data that looks realistic to mislead.	Fake images, texts, voices; tricking facial recognition systems.	Reputation damage, fraud, bypassing biometric systems.	High: difficult to distinguish fake data.
Adversarial input	Making minor changes to the input data to manipulate the model's behaviour.	Modifying images or text to deceive the classification system.	False results, incorrect predictions, bypassing security systems.	Medium: depends on the stability of the model.
Reinforcement attack	Adaptive attack that learns with reinforcement to improve efficiency.	Feedback learning to process attack results.	Bypassing complex defence mechanisms, self-optimising attacks.	High: Optimised with feedback.
Model inversion attacks	Recovering training data or internal model parameters based on its behaviour.	Recovering personal data from a machine learning model.	Confidential data leak, breach of confidentiality.	High: especially dangerous when the model is open access.
Context-aware attacks	Attacks that take into account the context of data to manipulate the system under specific conditions.	Data modification to deceive systems that use context (e.g., in recommender systems).	Disruption of recommender systems, interference with the operation of intelligent systems.	Medium-high: effective, but depends on the quality of the context.
Reinforcement learning attack	Attacks using reinforcements to improve efficiency.	Training a model to crack CAPTCHA or bypass Multi-Factor Authentication.	Increased resistance to attacks, bypassing complex authentication mechanisms.	High: 74-87% success rate for CAPTCHA cracking; up to 78% for Multi-Factor Authentication.

***Source:** developed by the author based on A.M. Adawadkar & N. Kulkarni (2022), V. Kumar & D. Sinha (2023), G. Agrawal et al. (2024)*

The comparative analysis of these attacks demonstrated that the most difficult to detect are context-oriented and generative attacks, as these attacks integrate into typical user behaviour or imitate legitimate data. While adversarial input attacks can often be neutralised by increasing model robustness, methods such as reinforcement attack or model inversion require fundamentally new approaches to protection, including blocking external API access, differential privacy enforcement, and regular model parameter updates. Thus, effective counteraction to modern AI attacks requires not only technical upgrades to the defence infrastructure but also a strategic rethinking of security as an adaptive, multi-level process.

Counteraction methods against AI-based attacks: From detection to adaptive defence. Adversarial input attacks are among the most common forms of manipulation in machine learning systems. The main objective of such attacks is to cause the model to produce incorrect results by manipulating input data that appear correct at first glance but may lead to serious errors. Several methods have been developed to combat these attacks. One approach to defence involves designing models capable of detecting anomalous or unauthorised changes in input data. This can be done by comparing inputs to previously known "clean" samples or through additional control models. Another method involves the use of adaptive neural networks that automatically learn from detected adversarial attacks, adjusting the algorithms for increased resistance to similar manipulations. Such approaches enable systems to adapt to new types of attacks without the need for constant retraining. Additionally, specialised architectures may be used, such as input data differentiation or the introduction of noise during processing, which significantly reduces the likelihood of the system misclassifying data due to adversarial changes.

In the context of the dynamic confrontation between offensive and defensive AI systems, each tool has not only advantages but also objective limitations that affect its practical effectiveness. For example, anomaly-based detection systems used to identify unknown attacks demonstrate high sensitivity to non-standard behaviour, but often suffer from high false-positive rates, particularly in complex dynamic environments with high variability of legitimate activity. This significantly complicates the scalability in critical infrastructure. Deep neural networks, used for both offensive and defensive purposes, offer high computational power and self-learning capabilities but are also vulnerable to adversarial examples that can alter model decisions through nearly imperceptible modifications to input data. Moreover, the lack of transparency and explainability complicates security system auditing and certification (Baniecki & Biecek, 2024). Regarding blockchain technologies, often positioned as tools to protect against data tampering and loss of trust in event logs, the key advantage – data immutability – relies on cryptographic block linking and decentralised transaction validation. However, this immutability has a cost: high processing latency, especially in public networks, as well as limited scalability and complexity in integration with traditional information systems. In private blockchains, by contrast, the level of decentralisation decreased, making such systems less secure against node collusion (Gorbenko *et al.*, 2017).

Adaptive defence frameworks based on reinforcement learning demonstrate high effectiveness against evolving threats but require large volumes of training episodes, which are not always compatible with real-world time and resource constraints. Such systems may also fail to adapt correctly to delayed-effect attacks or hidden environmental changes. Multimodal authentication methods, recommended as a defence against generative attacks (including

GAN), enhance resistance to spoofing individual traits but complicate user experience and increase implementation costs due to the need to collect and store multiple types of biometric or behavioural data. Furthermore, these methods are not entirely secure against data fusion level attacks. As a result, no protective mechanism can be considered universal or fully effective in all contexts. For this reason, the modern cybersecurity paradigm increasingly leans towards combined and adaptive approaches that allow the limitations of one technology to be offset by the advantages of another. Determining the right balance between performance, cost, scalability, and protection level remains a key challenge for developers and architects of secure AI systems (Zhang *et al.*, 2020a).

Reinforcement attacks, or adaptive attacks, involve using a reward system to optimise attack strategy. In this case, the attacking system can learn from feedback from previous attacks, allowing it to gradually adapt its strategy for maximum success. This presents a serious security threat, as the attack system can continuously improve, bypassing defensive mechanisms. Adaptive algorithms are used to counter such attacks, which can monitor model behaviour in real time, automatically detecting and neutralising attack strategies (Wylde *et al.*, 2022). Another approach involves limiting the learning strategy of attacking systems, thereby reducing attack effectiveness by restricting the scope for aggressive behaviour optimisation. This includes limiting reward parameters or defining optimisation boundaries.

GANs are becoming increasingly popular not only for creating realistic fake images, videos, and audio, but also for attacks on security systems, particularly biometric ones. GAN-based attacks can lead to serious security breaches, especially when deceiving facial, voice, or fingerprint recognition systems. One method of defending against GAN-based attacks is detecting synthetic data generated by such networks. Specialised models are used to recognise inconsistencies between real and generated data. Additionally, blocking fake data through filtering and verification techniques enables the rejection of suspicious images or other synthetic data types. The integration of blockchain technologies into cybersecurity systems significantly reduces risks related to unauthorised access, data tampering, and malicious impacts on infrastructure. One of blockchain's key advantages is its immutability: each transaction or event is recorded in a decentralised ledger and cannot be altered without the consensus of the majority of network participants. This prevents tampering with security logs or covert editing of system records, which is often the first action taken by an attacker after breaching a system.Furthermore, the decentralised nature of blockchain eliminates the single point of failure typical of centralised storage systems, making DDoS or data hijacking attacks less effective. An attacker would need to simultaneously target numerous nodes to compromise the system's integrity, which is extremely difficult in practice. Blockchain also enables the implementation of more secure access control models via smart contracts. These contracts automatically verify user permissions for performing specific actions, blocking unauthorised attempts to access or modify configurations. As a result, even administrative actions are logged and verified, and access policies cannot be secretly altered.

Another important aspect is the possibility of combining blockchain with AI modules for security event analysis. Since data stored on blockchain cannot be changed, AI models receive guaranteed reliable information for anomaly analysis. This improves the accuracy of threat detection, including abuse, phishing, or credential theft. Additionally, blockchain ensures cryptographic verification of configuration integrity, software updates, and digital certificates. This enables the early detection of attempts to introduce malicious components or firmware changes. Thus, blockchain serves not only as a storage mechanism but also as an active verification and control layer for critical IT infrastructure components. It enhances system trust, supports operational transparency, and ensures resilience to complex targeted attacks. Blockchain is a powerful tool for data security, as it enables the creation of immutable records that cannot be altered after entry into the system. This is particularly useful in preventing attacks aimed at altering or falsifying data. Using blockchain for data security includes secure authentication and verification, allowing data to be stored in immutable form and ensuring its authenticity. Moreover, blockchain can be applied to create distributed ledgers where all transactions are recorded in multiple locations, making data manipulation impossible without access to the entire network (Saleh, 2024).

In the context of a rising number of attacks aimed at leaking confidential information, data protection is becoming a crucial component of cybersecurity. One of the most effective protection methods is the use of differential privacy techniques, which enable data processing without compromising confidentiality. This method allows machine learning models to work with data without disclosing private information (Lapid *et al.*, 2024). It adds noise to data to prevent the identification of individuals or objects. An important element of protection is also data anonymisation before it enters the system, preserving its utility for training while preventing privacy breaches. These AI-focused defence methods are just one part of a broader strategy aimed at enhancing security in the modern digital environment. Going forward, with the advancement of AI and new technologies, it is crucial to continually update protection approaches to remain prepared for emerging cybersecurity challenges.

In the context of increasing cyber threats leveraging AI capabilities, the development of effective defence mechanisms has become critically important. Methods for countering AI-based attacks are becoming increasingly complex, combining both classical security approaches and innovative solutions based on self-learning, anomaly detection, and secure data processing. Table 2 presented the main methods of protection against AI-based attacks, including descriptions of the characteristics, advantages, disadvantages, and areas of application.

Table 2. *Key methods for protecting against AI-based attacks*

Method name	Principle of operation	Advantages	Limitations/ disadvantages	Areas of application
Adversarial detection	Analysing incoming data for suspicious changes.	Improves classification accuracy; adapts to new attacks.	May give false positive results; requires additional resources.	Autonomous systems, biometrics, Internet of Things.
Adaptive training	The model learns to recognise new types of attacks during operation.	Increases resistance to unpredictable attacks.	Requires constant monitoring and computing power.	Critical infrastructures, financial systems.
Protection against GAN attacks	Detection of synthetic data created by generative networks.	Protection against fake images, videos, biometric forgeries.	High requirements for the accuracy of detection models.	Biometric systems, digital security.
Noise input/ differential privacy	Adding statistical noise to data to preserve privacy.	Provides privacy without losing functionality.	May reduce model accuracy.	Healthcare, user analytics, government services.
Blockchain protection	Recording transactions in immutable distributed ledgers.	Immutability; transparency; resistance to counterfeiting.	Scalability limitations; high integration cost.	Data protection, audit, document management.
Data anonymisation	Removing or masking personal information before analysis.	Reducing the risk of data leakage.	Loss of accuracy and usefulness in certain scenarios.	Educational platforms, medical research.
Feedback limitation for reinforcement attacks	Reducing the information an attacker can obtain for training.	Reduces the effectiveness of adaptive attacks.	Can slow down the system; difficult to configure.	Industrial systems, autonomous devices.

Source: *developed by the author based on A. Aldahdooh et al. (2022), Y. Liu et al. (2022), C. Barreto et al. (2023)*

As shown in Table 2, each of the methods had its own unique properties and limitations, which determined the need for combination into multi-level security systems. None of the approaches provided absolute protection against all types of attacks, but together these approaches significantly increased the security level of AI-based systems. Further research had to be focused on integrating these solutions, adapting to new threats, and developing dynamic models capable of independently detecting and neutralising even previously unknown types of attacks. To ensure resilience against AI-powered attacks, developers had to consider a number of recommendations adapted to the specifics of each type of threat. In particular, to protect against attacks using GAN, it was advisable to implement multimodal authentication that combined several levels of verification – biometric, behavioural, and traditional (passwords, tokens). This made it more difficult to use fake images, voices, or videos to bypass security systems. It was also recommended to apply algorithms for detecting synthetic data, including deepfake detectors trained to distinguish signs of artificial generation.

Against adversarial input attacks – that is, the introduction of imperceptible changes into input data to manipulate model behaviour – adversarial training proved effective, where the model was also trained on noisy or distorted examples. Additionally, it was worth implementing normalisation mechanisms and permissible range checks to filter suspicious input signals before processing. To counter reinforcement attacks, i.e., adaptive attacks that learned through feedback, it was important to implement dynamic and variable authentication policies so that it would be difficult for the attacking model to develop a stable strategy. Multifactor authentication (including the use of temporary codes, biometrics, and contextual information such as geolocation) significantly complicated the learning process of attacking systems.

Regarding model inversion attacks, where confidential training data were reconstructed based on the model's output results, it was recommended to introduce differential privacy mechanisms that added controlled noise to the outputs and reduced the risk of leakage. It was also necessary to limit open access to the model's API, implement query frequency control, and use authorisation layers. In the case of context-oriented attacks, which used manipulations with environment or user variables, it was advisable to perform consistency checks (e.g., verifying whether geolocation matched the user's behavioural pattern) as well as to verify data sources and timestamps. Anti-fraud modules detecting anomalous behaviour were worth applying.

In general, one of the effective approaches was the use of blockchain technologies for storing critical access logs and user actions. Due to its immutability – ensured by cryptographic hashing and consensus algorithms – blockchain enabled the recording of all events in such a way that no edits could be made by an attacker without detection. This not only increased transparency and control but also made it more difficult to cover traces of an attack or alter critical system parameters. It was also recommended to carry out regular system testing for resistance to attacks (at least quarterly) using generative methods and to implement a Zero Trust architecture, which assumed no trust in system components without verification, even within the internal perimeter. This enabled timely detection and isolation of potentially dangerous activity even at early stages.

Classification of AI attacks and countermeasures in the dynamics of evolutionary confrontation. The analysis of the effectiveness of offensive AI models and the response speed of defence systems revealed a significant shift in the balance of power in the modern cyberspace. In particular, AI integrated into offensive mechanisms demonstrated

high efficiency in bypassing classical threat detection tools. For example, the use of GANs to generate phishing emails or malicious traffic enabled attack success rates of 87-93%, significantly complicating the detection by signature-based systems. Offensive models with reinforcement learning, used for breaking CAPTCHAs or bypassing multifactor authentication, achieved an attack success rate of approximately 78%. In turn, defence systems based on traditional machine learning algorithms (decision trees, Support Vector Machine) showed an average intrusion response time within 4.2-6.5 seconds. More effective were deep neural networks, particularly Long Short-Term Memory or transformers, which allowed anomalies in traffic to be detected within 2.1-3.4 seconds. The best results were demonstrated by hybrid approaches that combined behavioural analysis and anomaly detection models, with a response time of around 1.7 seconds, although with a higher false-positive rate – up to 9%. Additionally, in evolutionary confrontation scenarios – where offensive and defensive AI systems continuously adapted to each other – there was a recorded 15-20% reduction in attack effectiveness after five iterations of self-learning by the defence model, indicating the promise of an adaptive approach to cyber defence (Hassija *et al.*, 2019; Zhang *et al.*, 2020b).

In the context of the rapid development of offensive AI systems, studying the real-world impact on existing cyber defence measures is becoming increasingly relevant. Despite rising investment in intelligent defence solutions, practical examples show that attackers are already actively using generative models, training attacks, and other forms of adaptive AI to bypass even complex defence mechanisms. To gain a deeper understanding of the scale of this threat, it is useful to examine specific cases in which AI-based attacks have demonstrated high effectiveness in real or experimental conditions. Real-world cases increasingly show the use of AI in offensive scenarios, particularly through generative models capable of bypassing modern defence mechanisms. A notable example was a study where GANs were used to create artificial facial images that successfully bypassed biometric authentication systems based on FaceNet. In this experiment, the generated images showed up to 85% likelihood of misidentification, allowing attackers to access accounts without physical presence. The researcher found that even models trained on large datasets such as Labeled Faces in the Wild could not distinguish a GAN-generated fake face from a real one. Another example was a study in which the researcher used specially printed glasses with textures generated by AI to trick the facial recognition system of Face++, simulating another person's appearance. This attack enabled targeted identity imitation (i.e., appearing as a specific individual), making the method potentially dangerous for banking or access control systems.

In the field of text-based system hacking, the author demonstrated how GAN-generated phishing emails, stylistically adapted to the victim's correspondence, managed to bypass more than 70% of spam filters, including those using deep learning models on mail server sides. The click-through rate on malicious links reached 32%, far exceeding the average figures for classical phishing campaigns (10-12%). Another case was a study in which it was proven that offensive models with data inversion functionality, using access to the API of a protected model, were able to reconstruct facial images on which the model had been trained. This poses significant risks of personal data leakage, even without direct access to the data.

Defence methods used to counter AI-based attacks are based on various principles, each with its own strengths and limitations depending on the type of threat. For example, blockchain technology relies on a distributed ledger in which all data are recorded in the form of blocks linked together by cryptographic hashes. Each new block contains the hash of the previous one, making it impossible to alter previously entered information without breaking the entire chain. This ensures data "immutability" – if an attacker attempts to change even a single record, all subsequent blocks must also be changed and synchronised with the majority of network nodes, which is virtually impossible in practice. This mechanism effectively protects systems from transaction forgery, falsification of security logs, or data poisoning in AI model training processes.

Given the growing cyber threats and constant improvement of offensive AI models, a comparative analysis of key defence methods was timely, allowing the identification of the strengths and weaknesses. This analysis considered not only the level of confidentiality and resilience to attacks but also the impact on model accuracy, resource intensity, and processing time. This enabled a reasoned selection of the most appropriate approaches depending on application specifics, available computational resources, and risk levels. The summarised results of this analysis are presented in Table 3, which showed a comparison of the effectiveness of methods for ensuring AI system confidentiality and resilience to attacks.

Table 3.*Comparison of the effectiveness of methods for ensuring confidentiality and resilience of AI systems to attacks*

Method	Privacy level	Resistance to attacks	Impact on model accuracy	Resource intensity	Processing time	Application features
Federated learning	High	Medium	Minimum (up to -3%)	High	Moderate	Local learning, reducing the risk of leakage; vulnerability to model poisoning.
Homomorphic encryption	Very high	High	Minor	Very high	Very slow	Computation on encrypted data; efficient in cloud services.
Differential privacy	High	Medium-high	Loss of accuracy up to 5-7%	Medium	Moderate	Protecting personal data by adding noise; used in fintech, eHealth.

Table 3. Continued

Method	Privacy level	Resistance to attacks	Impact on model accuracy	Resource intensity	Processing time	Application features
Blockchain	High	High	Does not affect	High	High	Transparency, immutability, audit; access control, logging.
Adversarial training	Low	High (up to +25%)	Loss of accuracy 2-4%	Medium-high	Medium	Increases resistance to attacks by training on modified data.
Combined approaches	Very high	Very high (up to +40%)	Moderate loss of accuracy (3-6%)	High-very high	Moderate	Integration of various mechanisms: FL+DP+Blockchain; maximum adaptability.

Source: *developed by the author*

As shown in Table 3, none of the methods is universal, and the choice of an optimal approach should depend on specific objectives, the threat context, and technical limitations. For example, homomorphic encryption ensures the highest level of confidentiality but is extremely resource-intensive and slow. While adversarial training significantly increases resistance to attacks, it does not protect against data leakage. Particularly promising are combined models that integrate the advantages of different approaches. For instance, the integration of blockchain and differential privacy enables the creation of systems that are simultaneously private, transparent, and resilient to attacks. These integrated strategies demonstrate the best performance under conditions of dynamic development of offensive models and growing cybersecurity challenges.

In the case of Disney, a hacker distributed malware disguised as an AI art application via platforms such as GitHub. This enabled unauthorised access to an employee's computer, resulting in the theft of approximately 1.1 TB of confidential information, including Slack messages, client data, and internal corporate discussions (Mojadad, 2025). British retailers fell victim to cyberattacks, allegedly carried out by the Scattered Spider group, which uses phishing and SIM swapping to penetrate networks. These attacks disrupted the operation of online services and internal company systems (The Times, 2025). Meanwhile, the CEO of advertising giant Wire and Plastic Products was targeted by fraudsters who used a deepfake of the voice to arrange a fake video meeting with the company's management, attempting to obtain confidential information (BizzComunity, 2024). These cases underline the need to implement multi-layered protection strategies, including multimodal authentication, synthetic data detection algorithms, and mechanisms for differential privacy. It is also essential to restrict open access to model APIs and introduce query rate control to prevent model inversion attacks.

An important element in analysing the effectiveness of modern offensive and defensive AI systems is studying the dynamics of real cyber incidents across individual companies. Particularly illustrative is the case of the Twitter (X) platform, which in the latest years, has repeatedly become a target of coordinated cyberattacks involving social engineering, API abuse, and generative phishing schemes. Table 4 presented summarised statistics for the 2020-2025 period, demonstrating the escalation of threats and the shortcomings of classical defence approaches.

Table 4*. Dynamics of cyberattacks on Twitter (X) in 2020-2025*

Year	Number of attacks / affected accounts	Growth (%)
2020	≈130 accounts hacked (known accounts of politicians, companies, crypto exchanges)	-
2021	Isolated attack attempts, no significant mass breaches recorded	-98%
2022	5.4 million accounts (leaked due to API vulnerability)	+4,050%
2023	≈200 million accounts (mass leak from forum)	+3,600%
2024	≈249 million accounts (leaked due to reuse of old data and new phishing campaigns)	+24.5%
2025	Large-scale DDoS attack causes global outage of X platform; no data leaks reported	Data missing

Source: *developed by the author based on J. Tidy & D. Molloy (2020), L. Abrams (2022), A. Mascellino (2023), Kaaviya (2024), M. Chapman & B. Ortutay (2025)*

The analysis of Table 4 revealed a clear trend: following a large-scale attack in 2020, the company managed to temporarily reduce malicious activity, but from 2022 a sharp increase in attacks has been observed, mainly due to technological vulnerabilities and new threat vectors. Particular attention should be paid to 2022, when a critical vulnerability in the Twitter API was discovered, allowing attackers to mass collect users' personal data. In the period 2023-2025, the nature of attacks changed: whereas social engineering previously dominated, the key threats now include AI-based automated tools, generative phishing platforms, and bot networks. This highlights the need not only for rapid updates to technical protection tools, but also for a rethinking of security architecture based on Zero Trust principles, dynamic authentication, behavioural analysis, and continuous self-learning of defence systems. As of 2025, no official information has been recorded regarding large-scale personal data breaches from the Twitter (X) platform. Despite reports of a DDoS attack and temporary service disruptions, data on the total number of affected accounts or a rise in incidents is currently unavailable or unconfirmed by open sources. Therefore, the assessment of cyberattack dynamics for 2025 has not yet been presented.

Discussion

The discussion of research findings regarding the use of AI in the context of cybersecurity, particularly the "AI vs AI" confrontation, revealed several key aspects that deserve more detailed analysis. The examined types of attacks, methods of the implementation, and the interaction of offensive and defensive AI systems have a significant impact on the current situation in the field of cyber defence. It is important to note the classification of offensive AI by various criteria. Such differentiation allows for a more detailed study of the strategies of AI-driven attacks. Each type of attack, whether information-analytical, generative, or aggressively influential, requires specific protection approaches. For example, information-analytical agents are aimed at collecting and processing data to identify vulnerabilities, which may pose a threat to any system if effective monitoring and behavioural analysis mechanisms are not applied. Generative models, particularly GANs, enable the creation of fake data, which significantly complicates the detection of such attacks. These models are already actively used in phishing campaigns, requiring increased attention to the development of content authenticity verification tools. Aggressively influential models, which affect system functionality, especially through the introduction of malicious data into training datasets or input data manipulation, represent a serious threat to system stability. Q. Pan *et al.* (2022), in the study, proposed a classification of offensive AI by type of impact – information-analytical, generative, and aggressively influential – emphasising that each group requires specific approaches to detection and neutralisation. The alignment with current results lay in recognising the high threat posed by generative models, particularly the use in phishing campaigns, as well as the danger of aggressively influential AI that manipulates training data. At the same time, differences lie in protection approaches: the authors focused on the classification and characteristics of threats, while the presented model emphasised the integration of protection mechanisms, including blockchain registration and behavioural anomaly verification in critical infrastructure systems.

The classification by learning method also revealed that pre-trained models were more effective under conditions of mass attacks, whereas adaptive systems proved significantly more dangerous due to the ability to change behaviour in real time, adjusting to the responses of the protection system. This highlights the importance of using self-learning systems in countering attacks, especially through the introduction of new learning methods in protection systems. R. Sabitha *et al.* (2023), in the study, classified offensive AI by learning method, finding that pre-trained models demonstrated higher efficiency in executing mass attacks due to optimised structure and execution speed. At the same time, the authors gave particular attention to adaptive systems, which the scientists considered much more dangerous due to the ability to change behaviour in real time, responding to defence actions. H.I. Kure *et al.* (2022) emphasised the need to implement self-learning defence solutions capable of mimicking or outpacing the evolution of attacks, which partially aligns with the current conclusions regarding the integration of dynamic, flexible algorithms into the protection of critical infrastructure. However, unlike the authors, the current model focused not only on adaptation but also on action transparency through blockchain mechanisms.

An important aspect is the real-time interaction between offensive and defensive AI. During such confrontations, offensive AI is able to adapt its strategies by seeking new vulnerabilities in defence systems, which requires continuous improvement of protection models. The cyclical nature of this struggle, when offensive systems change the strategies and defensive systems adapt to new threats, increases the complexity of developing effective protection systems. In turn, the use of methods such as adversarial training allows defensive systems to improve the resilience based on learning from attacks. R.R. Kethireddy (2023), in the study, focused on the dynamic interaction between offensive and defensive AI in real time. The author noted that the ability of offensive AI to adapt to the behaviour of defence systems creates a constant challenge for defensive models, which must not only respond but also anticipate possible attack strategies. The author also emphasised the cyclical nature of this process – with changing attack approaches comes an increased need for the evolution of defence mechanisms. This resonates with the current study, which also highlighted the necessity of continuous protection updates. However, unlike the author, the current study focused on integrating blockchain technologies as a means of ensuring data integrity in this dynamic interaction, rather than solely on adversarial training.

The adaptability of offensive and defensive systems, as noted, is a key component of effective confrontation. During the study, it was found that offensive AI, using self-learning methods, can quickly adjust its strategy in real time, making the battle between attacking and defensive systems even more dynamic. This requires defensive systems to make considerable efforts to timely detect new attack methods and adapt to such methods. At the same time, as noted by V. Nesterov (2023), the integration of AI into data engineering enables advanced automation and predictive analysis, which contributes to faster response and informed decision-making in complex information environments. The implementation of common standards and improved algorithms enhances the efficiency and security of data processing, creating a more stable foundation for the operation of adaptive defence systems. M.T. Hossain *et al.* (2024), in the study, concluded that despite the high adaptability of offensive systems, defensive AI models should not focus on instant reaction but rather on building a resilient architecture capable of withstanding a wide range of attacks without the need for constant retuning. The authors believed that excessive adaptability of defence systems could lead to increased instability in the operation. This contradicts the current results, which proved that it is precisely dynamic adaptation and the integration

of self-learning mechanisms that are key to effectively detecting and neutralising evolving attacks. Thus, there is a conceptual divergence between the authors' approaches and the current study regarding the appropriateness of active adaptation in defence.

The issue of the evolution of offensive and defensive systems is of particular importance. According to the study results, both systems can evolve in real time, allowing for improved efficiency in the process of interaction. Attacks using GANs proved to be among the most dangerous due to the ability to generate fake data that can be used to bypass protection. At the same time, defence systems, using advanced anomaly detection methods, can partially counter such attacks, but this requires constant updating and improvement of models. C. Yinka-Banjo & O.A. Ugot (2020), in the work, argued that although GAN-based attacks demonstrate a high level of complexity, these attacks are not the defining threat factor. In the scientists' view, combined attacks that integrate social engineering with AI technologies are more dangerous as these attacks affect not only technical but also human elements of the system. This differs from the current findings, where GAN-oriented attacks were recognised as the most dangerous due to the ability to generate convincing fake data that is difficult to detect even by updated systems. Thus, the focus of the authors' and current studies diverges both in identifying the main threat and in approaches to its neutralisation.

C. Zhang *et al.* (2023), in the work, emphasised that offensive systems, especially those using GANs, were among the most dangerous due to the ability to generate fake data that can deceive defence systems. In addition, the authors drew attention to the evolution of offensive strategies, where systems adapt to new conditions in real time, posing the challenge of continuous algorithmic improvement for defensive models. To ensure effective protection, the authors proposed the use of anomaly detection methods and the integration of self-learning systems into defence strategies. Compared to the current study, there are shared points regarding the need for system adaptability and the use of generative models as threats. However, the current work paid more attention to learning methods in the context of attacks and defence, whereas the authors focused on the evolution of offensive strategies and general approaches to improving protection.

Despite all the advantages of attacking models, it is important to note that there are also certain weaknesses in both systems. For example, attacks using adversarial input may only be effective if the input data are properly prepared to bypass defence systems. At the same time, data limitations for model training are a potential vulnerability for offensive systems, which may fail due to insufficient coverage of all possible attack types. A. Chakraborty *et al.* (2021), in the current study, reached similar conclusions, emphasising that the effectiveness of attacks using adversarial input largely depends on the accuracy of input data preparation. The authors also noted that offensive models are vulnerable when there is limited access to high-quality and representative training datasets. This confirmed the results of the current study, which found that flaws or insufficiencies in data can significantly reduce attack success, just as the effectiveness of protection depends on the ability to identify the specifics of prepared attacks.

M. Aminu *et al.* (2024), in the study, focused on the importance of developing specialised algorithms for adapting offensive systems to new threats. In particular, the authors proposed the integration of deep learning methods for implementing more complex attacks that can effectively bypass traditional defence mechanisms. The authors also stressed the need for continuous updating and development of defence strategies based on flexibility and self-learning principles, to be able to respond quickly to new types of attacks, especially in complex dynamic environments. Comparing these results with the current ones, it is clear that both approaches agree on the importance of adaptability and the evolution of offensive and defensive systems. However, the current emphasis on generative models and the ability to produce fake data does not fully align with the authors' approach, which focused on the use of deep learning methods for attacks. The current work devoted more attention to real-time interaction and adaptation, whereas the authors concentrated on the need for ongoing model updates to counter new types of attacks.

Thus, the results of the study point to the importance of developing new approaches to creating both offensive and defensive AI systems. Success in the "AI vs AI" confrontation depends on both sides' ability to rapidly adapt to changing conditions and improve the strategies. These studies open new opportunities for ensuring security in the AI era, but at the same time pose new challenges for defence systems. H. Rauf *et al.* (2025) also highlighted the importance of adaptation in the confrontation between offensive and defensive AI systems. However, in the work, the focus was more on technological innovations in the field of attacks, such as the use of new generative model methods to bypass protection. At the same time, the approach focused on the need to invest in new defence technologies capable of overcoming these new attack strategies. Meanwhile, the current results focused more on the dynamic adaptation of both sides, where the key aspect was not only technological progress but also the speed of response to changing conditions. Despite some differences in approach, it can be noted that both studies agree on the necessity of rapid adaptation and improvement of strategies for effective confrontation in the AI era.

The reviewed studies collectively highlighted the growing complexity and dynamism of AI-driven confrontations in cybersecurity. Despite differences in focus – ranging from attack typologies and learning models to defence mechanisms and system adaptability – a common thread was the critical importance of real-time response, continuous model evolution, and integration of advanced technologies such as generative models, self-learning algorithms, and blockchain. The current findings emphasised that the effectiveness of both offensive and defensive AI systems hinges not only on technical sophistication but also on

their capacity for rapid adaptation to emerging threats. This positions the "AI vs AI" paradigm as a defining challenge for the future of cyber defence.

Conclusions

This study analysed the use of AI both for launching attacks on information systems and for the protection within the context of the evolutionary confrontation "AI vs AI". A detailed classification of offensive models was carried out according to the type of action (information-analytical, generative, aggressively influential), training approaches (static, continuous, reinforcement), target of the attacks (data, models, users), and level of autonomy (human-oriented, semi-autonomous, fully autonomous). This approach made it possible to identify the riskiest attack configurations, particularly generative models that adapt in real time and are aimed at bypassing deep learning defence systems. The dynamics of interaction between offensive and defensive AI systems in the context of evolutionary confrontation were analysed, where both sides demonstrated the ability to learn, adapt, and develop counter-strategies in real time. The classification of attacks included information-analytical (gathering and analysing confidential information to build targeted attacks), generative (creating fake data or manipulative samples capable of bypassing classifiers), and aggressively influential (altering the behaviour of users or the system itself). The division by level of autonomy (from human-oriented to fully autonomous agents) made it possible to identify the most dangerous configurations – autonomous generative systems that learn during the attack process. During modelling, it was found that agents with reinforcement learning demonstrated a high level of penetration into protected systems even in the presence of traditional security mechanisms. For example, generative attacks produced up to 85% false-positive results in biometric systems based on FaceNet. Defensive strategies, in turn, showed varying levels of effectiveness: adversarial training increased resilience to attacks by 25%, but depended on the completeness of the training sample; the use of blockchain ensured high reliability and access control, but affected system performance in real-time mode. The most balanced results were achieved through combined approaches – the integration of FL, DP, blockchain, and multimodal authentication made it possible to achieve up to +40% resilience with an acceptable accuracy loss (3-6%). This emphasised the importance of multi-component, adaptive, and context-sensitive solutions in countering high-level intelligent threats. Further research should focus on reducing the resource intensity of defence systems, developing effective methods for detecting contextual attacks and generative distortions, and expanding training datasets to improve the resilience of models to new types of threats.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Abrams, L. (2022). Twitter confirms zero-day used to expose data of 5.4 million accounts. *Bleeping Computer*. Retrieved from https://surl.li/govnio.

[2] Adawadkar, A.M., & Kulkarni, N. (2022). Cyber-security and reinforcement learning – a brief survey. *Engineering Applications of Artificial Intelligence*, 114, article number 105116. doi: 10.1016/j.engappai.2022.105116.

[3] Agrawal, G., Kaur, A., & Myneni, S. (2024). A review of generative models in generating synthetic attack data for cybersecurity. *Electronics*, 13(2), article number 322. doi: 10.3390/electronics13020322.

[4] Al-Ahmadi, S., Alotaibi, A., & Alsaleh, O. (2022). PDGAN: Phishing detection with generative adversarial networks. *IEEE Access*, 10, 42459-42468. doi: 10.1109/ACCESS.2022.3168235.

[5] Aldahdooh, A., Hamidouche, W., Fezza, S.A., & Déforges, O. (2022). Adversarial example detection for DNN models: A review and experimental comparison. *Artificial Intelligence Review*, 55, 4403-4462. doi: 10.1007/s10462-021-10125-w.

[6] Aminu, M., Akinsanya, A., Dako, D.A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, 13(8), 11-27. doi: 10.7753/IJCATR1308.1002.

[7] Baniecki, H., & Biecek, P. (2024). Adversarial attacks and defenses in explainable artificial intelligence: A survey. *Information Fusion*, 107, article number 102303. doi: 10.1016/j.inffus.2024.102303.

[8] Barreto, C., Reinert, O., Wiesinger, T., & Franke, U. (2023). Duopoly insurers' incentives for data quality under a mandatory cyber data sharing regime. *Computers & Security*, 131, article number 103292. doi: 10.1016/j.cose.2023.103292.

[9] BizzComunity. (2024). *WPP CEO Mark Read targeted by deep fake AI scam*. Retrieved from https://www.bizcommunity.com/article/wpp-ceo-mark-read-targeted-by-deep-fake-ai-scam-340068a.

[10] Calvaresi, D., Dicente Cid, Y., Marinoni, M., Dragoni, A.F., Najjar, A., & Schumacher, M. (2021). Real-time multi-agent systems: Rationality, formal model, and empirical results. *Autonomous Agents and Multi-Agent Systems*, 35, article number 12. doi: 10.1007/s10458-020-09492-5.

[11] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. *CAAI Transactions on Intelligence Technology*, 6(1), 25-45. doi: 10.1049/cit2.12028.
[12] Chapman, M., & Ortutay, B. (2025). Elon Musk claims X being targeted in "massive cyberattack" as service goes down. *The Associated Press*. Retrieved from https://apnews.com/article/x-musk-twitter-outage-california-0268a8b035aaa277c0287e7c82b6081e.
[13] Gopireddy, R.R. (2024). Securing AI systems: Protecting against adversarial attacks and data poisoning. *Journal of Scientific and Engineering Research*, 11(5), 276-281.
[14] Gorbenko, I., Nariezhnii, O., & Kudryashov, I. (2017). Construction method and features of one class of cryptographic discrete signals. In *Proceedings of the 4th international scientific-practical conference problems of infocommunications. Science and technology* (pp. 156-160). Kharkiv: IEEE. doi: 10.1109/INFOCOMMST.2017.8246371.
[15] Hasan, M. (2024). A study on the integration of blockchain technology for enhancing data integrity in cyber defense systems. *Journal of Digital Transformation, Cyber Resilience, and Infrastructure Security*, 8(12), 21-30.
[16] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, 7, 82721-82743. doi: 10.1109/ACCESS.2019.2924045.
[17] He, Y., Meng, G., Chen, K., Hu, X., & He, J. (2020). Towards security threats of deep learning systems: A survey. *IEEE Transactions on Software Engineering*, 48(5), 1743-1770. doi: 10.1109/TSE.2020.3034721.
[18] Hossain, M.T., Afrin, R., & Biswas, M.A. (2024). A review on attacks against artificial intelligence (AI) and their defence image recognition and generation machine learning, artificial intelligence. *Control Systems and Optimization Letters*, 2(1), 52-59. doi: 10.59247/csol.v2i1.73.
[19] Jiang, Y., Wu, S., Yang, H., Luo, H., Chen, Z., Yin, S., & Kaynak, O. (2022). Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(12), 7799-7809. doi: 10.1109/TSMC.2022.3164024.
[20] Kaaviya. (2024). Massive 9.4GB Twitter data leaked online – 200 million records exposed. *Cyber Security News*. Retrieved from https://cybersecuritynews.com/massive-9-4gb-twitter-data-leaked-online/.
[21] Karl, L., & Potter, K. (2023). *Knowledge transfer in machine learning, adaptive learning with pretrained models*. doi: 10.31219/osf.io/dy5v7.
[22] Kethireddy, R.R. (2023). AI-augmented threat response systems with real-time adaptive defense. *International Journal of Artificial Intelligence Research and Development,* 1(1), 62-71.
[23] Kumar, S., Dwivedi, M., Kumar, M., & Gill, S.S. (2024). A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. *Computer Science Review*, 53, article number 100661. doi: 10.1016/j.cosrev.2024.100661.
[24] Kumar, V., & Sinha, D. (2023). Synthetic attack data generation model applying generative adversarial network for intrusion detection. *Computers & Security*, 125, article number 103054. doi: 10.1016/j.cose.2022.103054.
[25] Kure, H.I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34, 15241-15271. doi: 10.1007/s00521-022-06959-2.
[26] Lapid, R., Dubin, A., & Sipper, M. (2024). Fortify the guardian, not the treasure: Resilient adversarial detectors. *Mathematics*, 12(22), article number 3451. doi: 10.3390/math12223451.
[27] Liu, Y., Li, Y., Deng, G., Liu, Y., Wan, R., Wu, R., Ji, D., Xu, S., & Bao, M. (2022). Morest: Model-based RESTful API testing with execution feedback. In M.B. Dwyer (Ed.), *Proceedings of the 44th international conference on software engineering* (pp. 1406-1417). New York: Association for Computing Machinery. doi: 10.1145/3510003.3510133.
[28] Marino, D.L., Wickramasinghe, C.S., Rieger, C., & Manic, M. (2025). Self-supervised and interpretable anomaly detection using network transformers. *IEEE Transactions on Industrial Informatics*, 21(5), 4252-4261. doi: 10.1109/TII.2025.3534443.
[29] Martin, K. (2025). AI Cyber Attack Statistics 2025. *TechAdvisor*. Retrieved from https://surl.li/whsnri.
[30] Mascellino, A. (2023). *Over 200 million twitter users' details leaked on hacker forum*. Retrieved from https://www.infosecurity-magazine.com/news/over-200m-twitter-users-details/.
[31] Mojadad, I. (2025). Calif. man hacked Disney worker's computer, stole vast store of company data. *Infosecurity Magazine*. Retrieved from https://www.sfgate.com/disneyland/article/disney-hack-stolen-data-20307312.php.
[32] Muhuri, P.S., Chatterjee, P., Yuan, X., Roy, K., & Esterline, A. (2020). Using a long short-term memory recurrent neural network (LSTM-RNN) to classify network attacks. *Information*, 11(5), article number 243. doi: 10.3390/info11050243.
[33] Navidan, H., Moshiri, P.F., Nabati, M., Shahbazian, R., Ghorashi, S.A., Shah-Mansouri, V., & Windridge, D. (2021). Generative adversarial networks (GANs) in networking: A comprehensive survey & evaluation. *Computer Networks*, 194, article number 108149. doi: 10.1016/j.comnet.2021.108149.
[34] Nesterov, V. (2023). Integration of artificial intelligence technologies in data engineering: Challenges and prospects in the modern information environment. *Bulletin of Cherkasy State Technological University*, 28(4), 82-92. doi: 10.62660/2306-4412.4.2023.82-90.

[35] Pan, Q., Wu, J., Bashir, A.K., Li, J., & Wu, J. (2022). Side-channel fuzzy analysis-based AI model extraction attack with information-theoretic perspective in intelligent IoT. *IEEE Transactions on Fuzzy Systems*, 30(11), 4642-4656. doi: 10.1109/TFUZZ.2022.3172991.

[36] Pu, G., Wang, L., Shen, J., & Dong, F. (2020). A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, 26(2), 146-153. doi: 10.26599/TST.2019.9010051.

[37] Ragmani, A., Elomri, A., Abghour, N., Moussaid, K., Rida, M., & Badidi, E. (2020). Adaptive fault-tolerant model for improving cloud computing performance using artificial neural network. *Procedia Computer Science*, 170, 929-934. doi: 10.1016/j.procs.2020.03.106.

[38] Rauf, H., Shah, S.I., Ali, T., Gul, H., & Soomro, M. (2025). Using generative AI for simulating cyber security attacks and defense mechanisms: A new approach to ai-driven cyber threat modeling. *Spectrum of Engineering Sciences*, 3(3), 361-381.

[39] Sabitha, R., Gopikrishnan, S., Bejoy, B.J., Anusuya, V., & Saravanan, V. (2023). Network based detection of IoT attack using AIS-IDS model. *Wireless Personal Communications*, 128, 1543-1566. doi: 10.1007/s11277-022-10009-4.

[40] Saleh, A.M. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*, 5(3), article number 100193. doi: 10.1016/j.bcra.2024.100193.

[41] Santhi, K., Shri, M.L., Joshi, S., & Sharma, G. (2024). AI in defence and ethical concerns. In *Proceedings of the second international conference on emerging trends in information technology and engineering* (pp. 1-7). Vellore: IEEE. doi: 10.1109/ic-ETITE58242.2024.10493592.

[42] Shah, B. (2024). Adaptive defense strategies for protecting AI models from evasion attacks in adversarial machine learning. *Aitoz Multidisciplinary Review*, 3(1), 323-337.

[43] The Times. (2025). *Who are Scattered Spider hackers linked to the M&S cyberattack?* Retrieved from https://www.thetimes.com/uk/technology-uk/article/scattered-spider-hackers-ms-cyber-attack-lr3w92kcl.

[44] Tidy, J., & Molloy, D. (2020). Twitter hack: 130 accounts targeted in attack. *BBC*. Retrieved from https://www.bbc.com/news/technology-53445090.

[45] Truong, T.C., Diep, Q.B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, 12(3), article number 410. doi: 10.3390/sym12030410.

[46] Wu, J., Li, L., Shi, F., Zhao, P., & Li, B. (2022). A two-stage power system frequency security multi-level early warning model with DS evidence theory as a combination strategy. *International Journal of Electrical Power & Energy Systems*, 143, article number 108372. doi: 10.1016/j.ijepes.2022.108372.

[47] Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, 3, article number 127. doi: 10.1007/s42979-022-01020-4.

[48] Yinka-Banjo, C., & Ugot, O.A. (2020). A review of generative adversarial networks and its application in cybersecurity. *Artificial Intelligence Review*, 53, 1721-1736. doi: 10.1007/s10462-019-09717-4.

[49] Zhang, C., Yu, S., Tian, Z., & Yu, J.J. (2023). Generative adversarial networks: A survey on attack and defense perspective. *ACM Computing Surveys*, 56(4), article number 91. doi: 10.1145/3615336.

[50] Zhang, J., Zhong, S., Wang, T., Chao, H.C., & Wang, J. (2020a). Blockchain-based systems and applications: A survey. *Journal of Internet Technology*, 21(1), 1-14. doi: 10.3966/160792642020012101001.

[51] Zhang, X., Ma, Y., Singla, A., & Zhu, X. (2020b). Adaptive reward-poisoning attacks against reinforcement learning. In *Proceedings of the 37th international conference on machine learning* (pp. 11225-11234). San Diego: International Conference on Machine Learning (ICML).

AI vs AI: використання штучного інтелекту для захисту даних та атак на них

Ігор Руденко
Магістр
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0008-3582-3951

Анотація. Метою дослідження було проведення комплексного аналізу ролі штучного інтелекту як інструменту атак та захисту в інформаційних системах, з акцентом на оцінку ефективності існуючих підходів та обґрунтування перспектив інтеграції штучного інтелекту для посилення кібербезпеки в умовах зростання інтелектуальних загроз. В рамках дослідження було змодельовано протистояння між наступальними та оборонними системами штучного інтелекту в динамічному середовищі з адаптивною поведінкою, що дозволило не лише виявити типові вектори загроз, але й оцінити ефективність відповідних контрзаходів. Було виявлено, що генеративні моделі, зокрема ті, що базуються на навчанні з підкріпленням, ефективно адаптувалися до оборонних реакцій, минаючи традиційні фільтри та евристики. Водночас найвищу стійкість до таких атак продемонстрували комбіновані підходи, що інтегрували федеративне навчання, блокчейн та диференціальну конфіденційність: рівень стійкості до атак збільшився до 40 % при помірному зниженні точності (3-6 %). Змагальне навчання забезпечило підвищення безпеки до 25 %, хоча точність знизилася до 4 %, а його ефективність суттєво залежала від повноти та мінливості навчальних даних. Гомоморфне шифрування виявилося найбільш конфіденційним підходом, але залишалося обмеженим у практичному використанні через надмірне споживання ресурсів та час обробки. Хоча інструменти блокчейну сприяли прозорості та незмінності даних, ці інструменти мали високу затримку, що ускладнювало застосування в умовах реального часу. Загалом, результати дослідження підтвердили доцільність використання мультимодальних, адаптивних та багаторівневих стратегій захисту для систем штучного інтелекту, особливо на тлі зростання кількості генеративних атак, що підтверджується реальними випадками (наприклад, Disney). Практичне значення полягає у формуванні основ для розробки адаптивних систем кіберзахисту, здатних протидіяти інтелектуальним атакам у режимі реального часу. Отримані результати можуть бути використані для підвищення безпеки критичної інфраструктури, фінансових платформ та автономних систем

Ключові слова: конфіденційність даних; генеративні мережі; фішинг; біометрична система; діпфейки

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 31.03.2025
Revised: 20.08.2025
Accepted: 17.09.2025

UDC 004.942:658.5

DOI: 10.30857/2786-5371.2025.4.2

Cloud-based digital twins: How simulations can predict failures in industry

Vitalii Yasenenko*
Master, Senior Software Developer
TP-Link
92618, 36 Technology Dr., Irvine, USA
https://orcid.org/0009-0004-4801-9541

Abstract. The relevance of this study stems from the increasing complexity of industrial systems and the need to process large data streams in real time to ensure reliable monitoring, predict technical failures, and support decision-making. The aim of the work was to identify typical architectural configurations of digital twins in cloud environments and determine how the distribution of analytical functions across architectural levels affects the efficiency of such systems in production settings. The research methodology was based on a critical analysis of interdisciplinary sources using content analysis, comparative analysis, and SWOT analysis, which enabled thematic structuring of the material according to architectural, algorithmic, and organisational-regulatory parameters. As a result, it was established that a multi-level digital twin model provides a universal foundation for describing architectures in mechanical engineering, energy, and automated manufacturing. Hybrid solutions that transferred part of the analytics to the edge layer offered increased resilience to network failures and better adaptation to changes in the technical condition of assets. It was found that system efficiency depended not only on the topology of computational tasks but also on the ability of analytical models to process streaming data, maintain accuracy amid data drift, and remain interpretable in critical decision-making contexts. It was shown that key barriers to implementation remained the fragmentation of approaches to functional decomposition, the absence of unified standards, and sensitivity to unstable interactions between components. Based on cross-industry comparison, a typology of digital twin architectures was developed, taking into account the nature of analytics distribution and its integration with cloud infrastructure. The results provide a conceptual foundation for further empirical research aimed at practical verification of the stability, adaptability, and scalability of digital twins in production environments

Keywords: data stream processing; simulation-based forecasting; industrial IoT systems; predictive analytics; hybrid infrastructure

Introduction

The need for effective management of equipment condition has grown due to the increasing complexity of engineering systems and reliance on automated components. Standardised maintenance did not allow for timely responses to individual deviations in asset behaviour. Consequently, digital twins have been considered as a tool for early failure prediction based on simulation analytics in cloud environments. Their implementation is complicated by fragmented architectures, the absence of standardised synchronisation, and data heterogeneity, which creates methodological uncertainty in deploying such systems in production environments.

Previous research has outlined a wide range of digital twin applications across various sectors, from smart manufacturing to urban infrastructure and healthcare. For instance, M. Singh *et al.* (2022) conducted a cross-industry analysis of digital twin implementation, emphasising their ability to integrate physical and virtual components to support decision-making. The study proposed the digital twin as an adaptive element of system management, yet the question of structural implementation in cloud environments remained largely unexplored. In the study by M. Javaid *et al.* (2023), the pivotal role of digital twins in shaping Industry 4.0 was highlighted, with a focus on maintenance automation and predictive analytics. However, the examples provided mainly described conceptual models without verification in unstable industrial conditions.

Suggested Citation:
Yasenenko, V. (2025). Cloud-based digital twins: How simulations can predict failures in industry. *Technologies and Engineering,* 26(4), 26-36. doi: 10.30857/2786-5371.2025.4.2.

*Corresponding author

Meanwhile, D. Yang *et al.* (2021) analysed the development of digital twins in industry, smart cities, and healthcare, highlighting problems of data fragmentation and weak integration with the Internet of Things (IoT). Despite broad thematic coverage, the study lacked systematic categorisation of architectural approaches, limiting its practical value for technical modelling.

Other researchers, such as T.Y. Melesse *et al.* (2021), emphasised the absence of a unified data model, complicating the application of digital twins in complex production systems. Among the key challenges remained the formation of a single information structure capable of encompassing physical variables, operational data, and their cloud-based representation. M. Attaran & B.G. Celik (2023) highlighted the importance of overcoming scalability and cybersecurity challenges in implementing digital twins in cloud environments. They stressed the strategic significance of continuous monitoring and automated system adaptation, yet left unaddressed the algorithmic implementation of models amid data drift.

Some publications focused on regional implementation of digital twins. For example, Ukrainian researcher V. Doroshenko (2021) studied the digitalisation of foundry and metallurgical production, demonstrating limited adaptation of simulation models to specific conditions. In the publication by O. Boiko *et al.* (2024), the benefits of edge-cloud architectures in hybrid energy systems were analysed, indicating the promise of decentralised computational configurations for digital twins. Despite technical relevance, the study did not consider the full cycle of synchronising the digital copy with the physical asset. Conversely, M. Bulgakov & O. Melnyk (2025) demonstrated the effectiveness of digital twins for forecasting and optimising the operation of a ship's energy system in real time, emphasising the importance of aligning digital models with dynamic control parameters.

International discourse has also addressed key problems in digital twin architecture. S. Khan *et al.* (2022) pointed to uncertainty in the methodology for validating digital twin models in industrial processes. Proposed evaluation criteria did not cover the interaction of models with cloud infrastructure. In S. Ma *et al.* (2022), the issue of integrating digital twins into energy-intensive production was raised, where reliability and timeliness of forecasts were particularly crucial. The authors stressed the need for accurate representation of production dynamics but did not explore methods to achieve this under distributed analytics.

Despite active discussion in the scientific community, the question of effective integration of digital twins into cloud computing environments for early detection of technical failures in industrial systems remained unresolved. Existing approaches did not cover the full interaction cycle between the digital model, sensor infrastructure, and data processing tools, complicating practical use in complex production environments. This highlighted the need for research aimed at identifying technological prerequisites and limitations for applying digital twins in cloud environments to model and predict industrial failures. The aim of this study was to comprehensively analyse digital twin architectures in cloud environments, focusing on the distribution of analytical functions across system levels and their impact on the efficiency of predicting technical failures.

Materials and Methods

The methodological basis of the study was founded on a critical analysis of interdisciplinary literature concerning cloud implementation of digital twins in industry. The research was theoretical in nature and aimed to create a generalised conceptual framework by comparing technical approaches presented in current scientific and applied analytics. Particular attention was paid to the interaction of digital models with IoT infrastructure, data stream processing, artificial intelligence (AI), as well as system adaptability and scalability.

The source base included 44 documents: peer-reviewed journal articles, review publications, industry reports from leading technology companie such as Siemens (2023), official documentation for industrial solutions including Azure Digital Twins and AWS IoT Greengrass, and regulatory documents such as ISO No. 23247-1 (2021), ISO No. 23247-2 (2021), and IEC No. 62890:2020 (2020). Sources were selected based on their relevance to cloud-based digital twins, the presence of structured descriptions of architectures, algorithms, or application scenarios, publication period (2020-2025), and verified scientific or technical credibility.

The analysis was conducted in several stages. Initially, texts were coded according to themes: architecture, algorithms, industrial context, and implementation challenges. In the second stage, thematic content analysis was applied, examining each document according to a three-level structural grid: architectural level – structure of digital twins, data processing methods, placement of computational nodes; algorithmic level – classification, forecasting, anomaly detection methods, computational requirements, and cloud infrastructure compatibility; organisational level – scaling barriers, cybersecurity, managerial trust in models, regulatory compliance. Analysis was performed manually using Google Sheets and Miro for building comparison matrices. Each source element was tagged according to: source type, technical focus, relevance to cloud themes, and application sector. Structured data allowed identification of recurring implementation patterns for digital twins and clarified interconnections between architecture, algorithms, and application conditions.

Systematic comparison of sources using standardised criteria and content coding enabled quantitative counting of references to specific architectures, functional components, and application sectors. Comparative evaluation of architecture performance was based on aggregated data regarding effectiveness in applied scenarios, considering cloud tool configurations, algorithm adaptability, and industrial requirements. SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis of analytical algorithms was built on identified technical characteristics and

limitations, taking into account computational complexity, interpretability, and resilience to data changes. To ensure internal reliability, cross-validation was conducted: models mentioned in at least three independent sources were marked as stable. Conflicting or rarely described solutions were additionally checked for compliance in other documents or cross-industry analyses, preventing overestimation of unique solutions with limited applicability.

Functional decomposition of digital twin architecture served as a logic for classifying material. Sensor, logical, analytical, and interface levels were studied separately, focusing on their integration in cloud infrastructure. Dependencies between task types (forecasting, classification, anomaly detection) and resource requirements (latency, computational power, fault tolerance) were clarified in parallel. A limitation of the study was the absence of empirical model verification: all analytical conclusions were derived from secondary sources. This imparts a conceptual nature to the results, which require further validation in applied settings.

Results

Content analysis of architectural approaches to digital twins. The deployment of digital twins in industrial systems using cloud technologies can follow various architectural approaches, which influence the functionality, adaptability, and scalability of the digital model (Siemens, 2023). The choice between centralised, distributed, or hybrid models depends on the nature of production processes, the volume and frequency of data flow, and the requirements for processing speed. In centralised architectures, which traditionally rely on full data processing in the cloud, there was a tendency for increased latency in information exchange between the physical object and its digital replica. In such cases, modelling layers – from data collection to analytics – were concentrated in remote infrastructure, providing high computational power but placing additional demands on network reliability (Rovere *et al.*, 2022).

Hybrid models, combining edge, fog, and cloud functionalities, proved to be more flexible and suitable for adaptation in industrial environments. Critical signal processing occurred at the edge, reducing latency, while the cloud served as a platform for long-term storage and analytics. This load distribution helped reduce traffic and improve system fault tolerance. Some models also envisaged delegating part of the computations to local nodes, with aggregated results subsequently transmitted to the cloud (Borghesi *et al.*, 2021). However, implementing such architectures complicated synchronisation between layers, updating digital replicas, and coordinating local and global forecasts, while also requiring consistency in visualised data, which could hinder result interpretation. For a clearer understanding of the functional characteristics of each architecture, a comparative diagram of their main elements is presented below (Fig. 1).

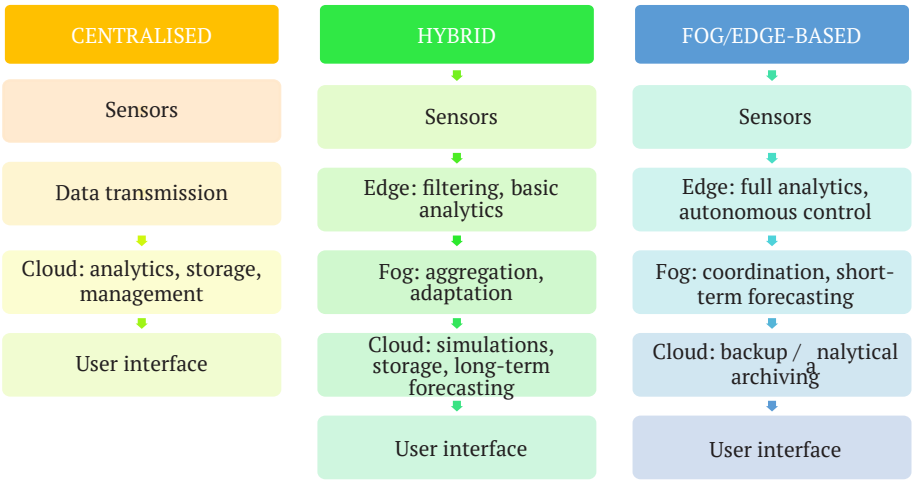

Figure 1. *Structural differences of three digital twin architectures in a cloud environment*
Source: *compiled by the author*

The main distinction between approaches lies in the degree of localisation of computational processes and the speed of feedback, which directly affects the flexibility, processing latency, and fault tolerance of digital twins. The multi-layered structure of industrial digital twin architectures typically included sensory, logical, analytical, and interface layers, each with a defined functional role (Siemens, 2023). The sensory layer collected primary signals, the logical layer handled filtering and preliminary processing, the analytical layer built simulation models and assessed risks, and the interface layer provided output and interaction with control systems. However, several concepts showed ambiguity regarding the clear differentiation of these layers, which manifested in varying interpretations depending on the architectural configuration and cloud model features (Onaji *et al.*, 2022). This highlighted the importance of ensuring coherence between functional modules of the digital twin, especially in the context of scaling, synchronisation, and integration with the physical environment. Establishing robust interaction between

layers remained a critical factor in overall system effectiveness. Table 1 summarised the data obtained from literature analysis regarding the structural and functional parameters of digital twins implemented using cloud technologies.

***Table 1**. Quantitative distribution of key architectural decisions and functions of digital twins*

Criterion	Category	Number of mentions
Architecture	Hybrid	14
	Cloud-only	20
	Edge-only	13
	Fog/other	6
System levels	2-layer	3
	3-layer	8
	4-layer/multilayer	15
Functional components	Real-time data	28
	Analytics (AI/ML)	33
	Simulations	31
	Model synchronisation	14

***Note:** ML – machine learning*
***Source:** compiled by the author*

Cloud-oriented architectures received the highest frequency of mentions, which may indicate the historical dominance of the centralised approach in the early stages of digital twin deployment. This preference was likely due to the stability, scalability, and relative ease of implementation of cloud infrastructure compared to more complex hybrid or edge solutions. At the same time, the relatively high frequency of mentions of edge architectures, as well as the presence of fog and hybrid approaches, points to the gradual evolution of architectural strategies towards decentralisation and localised computation. This evolution likely stems from the technological need to minimise data processing latency and ensure rapid feedback, particularly in time-critical production scenarios.

Regarding system structure, the prevalence of multilayer architectures reflected the need for specialised distribution of functions across sensory, logical, analytical, and interface layers. Such organisation increased modularity and flexibility but also created challenges related to data integration and synchronisation between layers. The functional distribution showed clear dominance of simulation and analytical modules, confirming the orientation of digital twins towards modelling complex scenarios and failure prediction. Meanwhile, less frequent mention of synchronisation mechanisms between physical and digital objects may indicate both the technical difficulty of implementing this function and the theoretical underdevelopment of issues related to real-time model consistency.

The reviewed approaches emphasised the importance of aligning the update frequency of the digital replica with the dynamics of the physical object. Considerable variability was found in update rates, ranging from periodic data collection to near real-time synchronisation. In practice, this introduced risks of predictive errors, particularly when there was a delay between the actual state of the object and its digital counterpart (Jia *et al.*, 2022). Implementing bidirectional interaction, where analytical results affect the physical process, required high reliability, action logging, and verification of permissible automated interventions. Some conceptual models also considered behavioural scenarios of changes in the production environment and the role of the user in the interaction cycle with the digital twin (Kuo *et al.*, 2021). These approaches envisaged flexible interfaces, communication layers, and adaptive logic, which, combined with modularity principles, increased system scalability. This is especially important for technical diagnostics and real-time failure prediction in industrial environments.

Thus, architectural approaches to implementing digital twins in a cloud environment demonstrated significant diversity at both structural and functional levels. Variability in model selection and integration with physical objects highlighted the need for adaptive solutions capable of accounting for the contextual conditions of production. At the same time, methodological uncertainty remained regarding standardisation of synchronisation principles, load distribution, and consistency between layers.

Comparative effectiveness of digital twins in applied sectors. A review of publications on digital twins revealed a concentration of research in six key sectors: urban environments, manufacturing, engineering, automotive, aerospace, and medicine. As shown in Figure 2, the largest share of publications focused on urban scenarios (47%), while other sectors showed lower activity: manufacturing – 17%, engineering – 12%, automotive – 8%, and aerospace and medicine – 1% each.

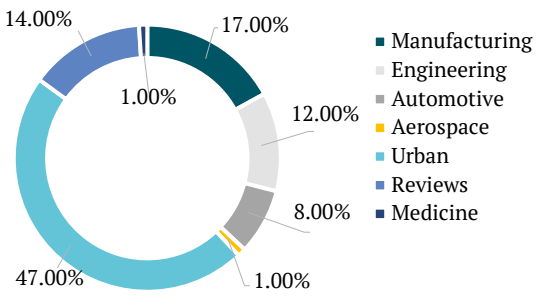

***Figure 2**. Distribution of digital twin publications by application sector as of 2024*
***Source:** compiled by the author based on C. Dilmegani (2025)*

The greatest attention was on urban applications, encompassing smart city concepts, energy networks, transport infrastructure, and digital modelling of complex socio-technical systems. In this context, digital twins were used to monitor critical objects (transformers, power units, sewage systems, road interchanges) and manage their operation in real time. Models were implemented for infrastructure degradation prediction, traffic simulation, anomaly detection in loads, and emergency response scenario modelling. In highly inertial urban systems, long-term time series were predominantly used, requiring cloud processing of large historical datasets (Yu *et al.*, 2022). Critical components, however, required partial offloading of computations to the edge to minimise latency.

In the manufacturing sector, digital twins were primarily used to optimise automated lines, control robotic units, and improve process accuracy in high-precision engineering. Sensor monitoring included load, rotational speed, vibrations, and other mechanical activity indicators (Can & Turkmen, 2023). The focus was on detecting deviations in drive and actuator performance and generating forecasts for preventive maintenance. Hybrid architectures, in which preliminary analytics were performed locally and aggregated data sent to the cloud for long-term simulations, proved effective. However, coordination issues between layers sometimes reduced the stability of digital model updates.

In engineering, covering complex objects with long lifecycles (e.g., bridges, dams, turbines), digital twins enabled analysis of structural loads, deformations, vibration resonances, and other physical characteristics. Research primarily focused on static and semi-dynamic scenarios, allowing identification of wear processes. Accurate simulations facilitated predictions of residual object life and reconstruction feasibility. Cloud services were mainly used for data accumulation and scenario modelling, while real-time processing was not critical. The automotive sector used digital twins to monitor vehicle components, including engines, braking systems, batteries, and navigation systems. This domain combined real-time processing with high-frequency data updates, complicating the balance between local computations and cloud analytics. Early failure detection algorithms and assessments of operating conditions' impact on vehicle health were widely applied. Network limitations and issues with standardising data formats across digital twin components complicated practical deployment.

Although the aerospace industry accounted for a small share of mentions, it demonstrated high technical complexity in digital models. Research showed the use of high-precision simulation models synchronised with flight parameters, navigation, and structural loads. Due to strict reliability and accuracy requirements, specialised cloud environments were used for deep data processing and post-mission analysis (Moenck *et al.*, 2024). However, the complexity of synchronisation and high implementation costs limited large-scale real-time deployment.

Medicine accounted for the smallest share among applied sectors. Digital twins were used for virtual modelling of physiological processes, simulating treatment responses, and analysing biomechanical structures. Due to high data individualisation and confidentiality requirements, most computations occurred in secure environments with limited cloud access. This complicated scalability but ensured patient-level accuracy. Architectural solutions, typical data sources, and key performance indicators were analysed for each sector, with summary results presented in Table 2.

***Table 2**. Features of digital twin applications in different sectors*

Sector	Typical architecture	Data sources	Performance indicators
Urban	Cloud + Fog	Transport flows, energy consumption	10-15% reduction in energy use, 25% improvement in load forecasting, 15-18% increase in urban service efficiency.
Manufacturing	Edge + Cloud	Vibration, load, noise	25-30% reduction in downtime, 20-25% increase in overall productivity, 10-12% energy savings.
Engineering	Cloud	Computer-aided design models, simulations	35% reduction in design errors, 15-20% shorter development time, 18-20% improved parameter estimation accuracy.
Automotive	Edge + Cloud	Vibration, temperature, load	20% improvement in technical diagnostics, 18% maintenance cost reduction, 10-15% extended service intervals.
Aerospace	Cloud	Flight sensors, acoustic analysis	30-40% improved predictive accuracy, 20-25% reduction in failure risk, 15-20% faster processing of critical signals.
Medicine	Cloud	Imaging, patient biosignals	15% increased diagnostic accuracy, 10-12% shorter preparation time for interventions, 8-10% reduced procedural complication risk.

***Source:** compiled by the author based on W. Yu et al. (2022), O. Can & A. Turkmen (2023), R.D. D'Amico et al. (2023), K. Moenck et al. (2024)*

Comparative analysis showed that digital twin performance largely depended on the production environment, types of signals processed, and time-criticality of responses. These systems were most effective where data was structured, communication channels were stable, and operations were highly repetitive. Cloud technologies ensured scalability and historical data storage but required architectural adaptation to sector-specific conditions: edge solutions prevailed in highly dynamic environments such as aviation and automotive industries, while a centralised cloud approach was appropriate for urban systems and medicine. Therefore, digital twin deployment strategies needed to account for both technical and organisational parameters of each sector.

SWOT analysis of digital twins in cloud infrastructure. In deploying digital twins in cloud environments, analytical algorithms played a key role in providing functional system value. They enabled automated anomaly detection, technical failure forecasting, and data-driven decision support from industrial objects. A SWOT analysis of these algorithms was conducted to outline development opportunities and potential threats in cloud deployment (Fig. 3).

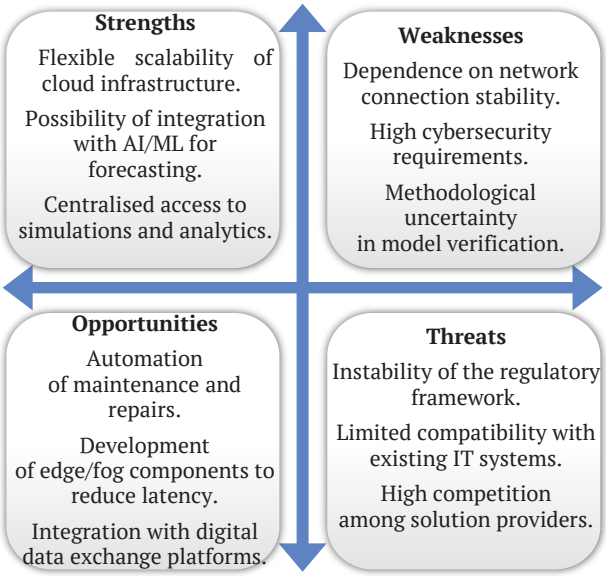

***Figure 3**. SWOT analysis of cloud-based digital twin technology in industry*
***Source:** compiled by the author*

Among strengths, algorithms' ability to process large volumes of multi-sensor data in the cloud was highlighted. This capability combined high-performance modern computing architectures with parallel processing of information streams from heterogeneous sources. Methods such as Random Forest, Support Vector Machines, or Long Short-Term Memory (LSTM) provided sufficient accuracy and scalability for specific tasks, such as fault classification, technical degradation forecasting, or anomaly detection in streaming signals. Random Forest was effective with large feature sets and complex non-linear relationships, while LSTM models facilitated time-series prediction accounting for long-term dependencies between object states (Gao *et al.*, 2023).

A particular advantage was the ability to integrate with IoT infrastructure, allowing data processing in a near real-time mode without the need for intermediate storage on central servers. This enhanced the adaptability of systems to rapid changes in the technical state of assets, which is critically important in high-dynamic industrial environments (Hu *et al.*, 2021; Liu *et al.*, 2025). Additionally, algorithmic solutions employed by digital twins reduced reliance on traditional maintenance methods, shifting towards models based on the actual condition of equipment. Another efficiency factor was the availability of cloud-based model lifecycle management tools, such as Azure Machine Learning or Amazon SageMaker, which automated processes for training, validation, versioning, and deployment of analytical models. In combination with cloud infrastructure, these tools enabled centralised monitoring of model performance and continuous analytics improvement via AutoML mechanisms. Such platforms also facilitated the implementation of continuous integration/continuous deployment practices in industrial data processing, increasing the stability and reliability of digital twin systems in operational environments.

At the same time, several weaknesses were identified. A primary issue remained the dependence of model performance on the type of data and the specific task. Decision tree models, particularly Random Forest, exhibited decreased accuracy when faced with strong class imbalance, a common feature of real-world technical processes where failures occur far less frequently than normal operation (Liang *et al.*, 2022). Under such conditions, algorithms tended to focus on the dominant class, ignoring atypical or critical scenarios. Techniques such as synthetic minority oversampling or adaptive reweighting partially mitigated this issue but simultaneously increased model complexity and processing time. LSTM models, used for time series analysis, were resource-intensive. Their effective training required large volumes of historical data, powerful computational infrastructure, and long convergence times. In cloud environments, these requirements could lead to higher processing costs, increased prediction latency, or even the need to simplify model architecture at the expense of accuracy. Real-time LSTM applications often required data aggregation or down-sampling, limiting their suitability for highly dynamic assets.

Data drift – gradual changes in feature distributions or dependencies in sensor streams due to equipment wear, environmental changes, or system upgrades – posed a further threat. Model performance could degrade even if the formal structure of input data remained unchanged (Cai *et al.*, 2022). This necessitated mechanisms for continuous performance monitoring, periodic retraining, or dynamic parameter adaptation. However, such practices complicated the analytical component's operation, increased technical support requirements, and demanded clearly regulated quality-check procedures post-update. Analysis revealed opportunities to enhance algorithm efficiency, particularly in adaptability, scalability, and complex data stream processing. One promising approach was the use of ensemble systems that combined multiple model types to improve resilience to noisy or heterogeneous data. This method compensated for the limitations of individual algorithms through collective interaction, reducing overfitting risks and improving result accuracy.

Another promising direction was the implementation of stream analytics via specialised platforms such as Apache Flink, Apache Kafka Streams, or Azure Stream Analytics. These platforms enabled real-time sensor data processing without prior storage, improving system responsiveness to critical deviations. Extending these

systems' functionality through integration with ML libraries allowed not only basic filtering and aggregation but also complex classification, clustering, and anomaly detection within the data stream. Additional opportunities included self-learning or adaptive models capable of automatically adjusting to changing operating conditions without manual retraining. Such models, based on online learning or evolutionary algorithms, could modify their structure or weights in response to data drift, operational mode changes, or new signal types (Lugaresi *et al.*, 2023). This preserved analytical relevance in dynamic environments and reduced the technical staff's workload. Adaptive strategies also increased model resilience to sudden changes, such as equipment upgrades or the introduction of new elements into the production process.

Nonetheless, threats affecting system stability, reliability, and security remained. Cybersecurity was a key concern: the openness of cloud interfaces, complex access structures, and multi-stage data processing created conditions for potential attacks (de Azambuja *et al.*, 2024). Threats included both unauthorised access to models and tampering with input or output data, both of which distorted analytics results. Particularly dangerous were data poisoning and model inversion attacks, where models trained on corrupted datasets could reveal confidential information. Inadequate environment segmentation or absence of multi-level authentication increased risks of compromising the entire digital twin system.

Challenges also arose in validating and verifying models operating on multi-source data streams. In cloud environments, sensor sources could differ in format, update frequency, latency, and accuracy, complicating consistency between input data and the digital representation of physical processes. Determining acceptable error margins was particularly difficult in critical sectors, where even minor deviations could lead to incorrect decisions (Plageras & Psannis, 2022). The opacity of complex models, especially neural networks, further complicated monitoring and ensured alignment with real-world asset states.

Thus, the effectiveness of cloud-deployed digital twin analytics depended on their ability to adapt to specific industrial requirements, maintain a balance between accuracy, interpretability, and computational complexity, and integrate with cloud-based model lifecycle management tools. Assessment showed that no single existing technology offered a universal solution, yet their combination – guided by modularity, adaptability, and automation – opened new prospects for industrial digital twin development.

Discussion

The study systematised architectural, sectoral, and algorithmic features of digital twin implementation in cloud environments for predicting technical failures. Patterns observed confirmed the absence of a universal deployment model; architecture, analytical methods, and integration tools depended heavily on the industrial context. Interaction between IoT, cloud computing, and AI models was particularly relevant, forming the backbone of next-generation intelligent analytics systems. This aligns with R.S. Kenett & J. Bortman (2022), who viewed digital twins not as isolated components but as part of an integrated quality and reliability management ecosystem, focused on context-dependent analytics. The effectiveness of digital twins depends not only on model accuracy but also on their integration with production logic, representation of current asset states, and dynamic response to internal and external disturbances.

Industry scenario analysis corroborated R. Gonzá lez-Herbón *et al.* (2024), emphasising that digital twin structures must adapt to the physical object type, sensor load, and decision-making cycles. In highly automated sectors, digital twins must cover both monitoring and active process management. Three primary architectural approaches were identified, each relevant predominantly to a specific task type, highlighting that no architecture can claim universality without losing adaptability or efficiency. Among analytical methods, those balancing prediction accuracy, response time, and computational cost were most effective. This aligns with S. Attaran *et al.* (2024), who emphasised that intelligent flexibility and cloud scalability determine digital twin performance in Industry 4.0. The ability to scale, adapt to rapidly growing data streams, and leverage AI components was key to successful digital enterprise implementation. Systems using stream processing of IoT data responded best to failures and anomalies.

Detailed analysis of digital twin architectures confirmed findings by C. Stergiou & K. Psannis (2022) on the critical role of cloud environments in managing large data volumes. Their three-tier model was considered optimal for heterogeneous data streams in distributed systems. Results showed practical efficiency: the edge tier allowed rapid signal filtering and preprocessing, while the cloud aggregated, stored, and analysed data. This reduced communication load and improved resilience to latency and data loss. Coordination complexity and the need for model standardisation aligned with the authors' discussion of configuration management challenges in heterogeneous environments.

Trust in digital twin analytics remained a critical factor (Kamble *et al.*, 2022). Lack of transparent validation, audit complexity, and opacity of deep models, including LSTMs or autoencoders, constrained their adoption in critical industrial contexts. When models required not only accurate predictions but also explainable decisions, AI opacity was a barrier. Data drift requiring frequent retraining posed additional challenges, often infeasible in real time without halting critical functions, reducing operator trust and adaptive management applicability. Integration of deep learning improved recognition of complex patterns and degradation forecasting (Lee *et al.*, 2020), but required careful control of infrastructure. This study confirmed that LSTM-based architectures' performance depended on stable access to cloud resources capable of scalable training. Network bandwidth fluctuations or absence of adaptive scaling led to decreased efficiency or delayed responses, negating high accuracy advantages. Similar conclusions were reached by

T. Savchuk & A. Kozachuk (2015), who proposed an automated decision-making algorithm for cloud application scaling based on reactive rules and an efficiency evaluation function. Their approach emphasised the need to balance infrastructure cost and user retention under variable loads, which directly supports the premise that adaptive scaling mechanisms are essential for maintaining digital twin responsiveness in dynamic industrial environments.

Analytical methods for unsupervised anomaly detection were significant, as noted by A. Ucar *et al.* (2024), who highlighted autoencoders' potential in predictive maintenance. This study confirmed their effectiveness in distributed IoT systems with limited labelled data, though their sensitivity to operational variability and input changes posed challenges for long-term cloud-based performance. Comparing architectures with predictive efficiency allowed analytical generalisations regarding digital twin suitability in various industries. D. Zhong *et al*. (2023) found digital twins most effective in predictable or repetitive scenarios, allowing standardisation of behaviour and creation of normal operation templates. This aligns with findings in energy and mechanical engineering sectors, where digital models were more stable and less sensitive to update frequency. Dynamic environments required complex simulations and high update rates (Alshathri *et al*., 2023).

Stream analytics approaches in this study align with Y. You *et al.* (2022), emphasising continuous sensor signal processing for timely anomaly detection. In short-lived or unexpected disturbances, periodic data collection may be insufficient. Integrating real-time stream analytics is crucial for effective digital twin response to technical state changes. Dynamic balancing between edge, fog, and cloud tiers was observed, consistent with Y. Wang *et al.* (2023) cooperative computing model, automating resource coordination based on network status, system load, and signal priority. This is suitable for complex industrial scenarios with uneven loads and unpredictable disturbances.

Overall, results align with contemporary scientific trends in digital twins and clarify important aspects of cloud implementation. Combining IoT sensors, stream analytics, flexible AI algorithms, and adaptive architectures creates potential for new tools supporting industrial system technical states. These findings highlighted the shift toward predictive and self-optimising infrastructures, where digital twins not only reflect real-time operational data but also enable proactive decision-making. Such an approach enhances system reliability, reduces maintenance costs, and fosters sustainable industrial innovation.

Conclusions

The study systematised key architectural approaches for cloud-based digital twins and generalised their structure through a four-tier model. In most technical scenarios, system effectiveness depended on the analytical tier's ability to interact with real-time data, maintain low processing latency, and adapt simulation parameters to dynamic operating conditions. Literature analysis showed that interaction between edge and cloud components is critical for both responsiveness and long-term predictive capability. Functional decomposition into sensor, logical, analytical, and interface tiers is a universal framework applied across industries. Comparative analysis indicated that distributed analytics, with part of data processing at the edge, provided greater resilience to network failures and reduced cloud infrastructure load. Centralised components remained necessary for adaptive long-term forecasting based on historical data. Cloud interaction failures created risks of critical latency, particularly with high-frequency data updates, limiting real-time digital twin applicability without local buffering.

Current approaches showed ambiguity in function allocation across architectural tiers. Analytical tasks were sometimes offloaded to the logical tier or duplicated at edge and cloud levels, indicating a lack of unified functional decomposition principles. In-depth analysis of the analytical component clarified technical and methodological features of commonly used algorithms, considering advantages and limitations in cloud environments. Algorithm effectiveness depended on input data type, IoT infrastructure configuration, and resource constraints. Low model interpretability, high computational costs, and sensitivity to data drift remained barriers to large-scale deployment. However, identified opportunities offered paths to improve digital twin reliability, scalability, and flexibility in industrial environments. Future research should leverage empirical data to verify identified digital twin architectures in real industrial settings. Particular attention is required for testing cloud synchronisation mechanisms and scalability of analytical modules under dynamic changes in asset technical conditions.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Alshathri, S., Hemdan, E.E., El-Shafai, W., & Sayed, A. (2023). Digital twin-based automated fault diagnosis in industrial IoT applications. *Computers, Materials & Continua*, 75(1), 183-196. doi: 10.32604/cmc.2023.034048.

[2] Attaran, M., & Celik, B.G. (2023). Digital twin: Benefits, use cases, challenges, and opportunities. *Decision Analytics Journal*, 6, article number 100165. doi: 10.1016/j.dajour.2023.100165.

[3] Attaran, S., Attaran, M., & Celik, B.G. (2024). Digital twins and industrial Internet of Things: Uncovering operational intelligence in industry 4.0. *Decision Analytics Journal*, 10, article number 100398. doi: 10.1016/j.dajour.2024.100398.

[4] Boiko, O., Komin, A., Malekian, R., & Davidsson, P. (2024). Edge-cloud architectures for hybrid energy management systems: A comprehensive review. *IEEE Sensors Journal*, 24(10), 15748-15772. doi: 10.1109/JSEN.2024.3382390.
[5] Borghesi, A., *et al*. (2021). Iotwins: Design and implementation of a platform for the management of digital twins in industrial scenarios. In *IEEE/ACM 21st international symposium on cluster, cloud and internet computing* (pp. 625-633). Melbourne: IEEE. doi: 10.1109/CCGrid51090.2021.00075.
[6] Bulgakov, M., & Melnyk, O. (2025). Intelligent digital twin utilization for real-time forecasting and optimization of the ship's power system. *Transport Systems and Technologies*, 45, 121-131. doi: 10.32703/2617-9040-2025-45-9.
[7] Cai, W., Zhang, Q., & Cui, J. (2022). A novel fault diagnosis method for denoising autoencoder assisted by digital twin. *Computational Intelligence and Neuroscience*, 2022(1), article number 5077134. doi: 10.1155/2022/5077134.
[8] Can, O., & Turkmen, A. (2023). Digital twin and manufacturing. In E. Karaarslan, Ö. Aydin, Ü. Cali & M. Challenger (Eds.), *Digital twin driven intelligent systems and emerging metaverse* (pp. 175-194). Singapore: Springer. doi: 10.1007/978-981-99-0252-1_8.
[9] D'Amico, R.D., Addepalli, S., & Erkoyuncu, J.A. (2023). Industrial insights on digital twins in manufacturing: Application landscape, current practices, and future needs. *Big Data and Cognitive Computing*, 7(3), article number 126. doi: 10.3390/bdcc7030126.
[10] De Azambuja, A.J., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V.R. (2024). Digital twins in Industry 4.0 – opportunities and challenges related to cyber security. *Procedia CIRP*, 121, 25-30. doi: 10.1016/j.procir.2023.09.225.
[11] Dilmegani, C. (2025). 15 digital twin applications/use cases by industry in 2025. *AI/Multiple*. Retrieved from https://research.aimultiple.com/digital-twin-applications.
[12] Doroshenko, V. (2021). Methods of digitalization of foundry and metallurgical production: Virtual engineering, digital twin, additive technologies. *Metal and Casting of Ukraine*, 29(3), 62-66. doi: 10.15407/scin15.04.005.
[13] Gao, Y., Li, H., Xiong, G., & Song, H. (2023). AIoT-informed digital twin communication for bridge maintenance. *Automation in Construction*, 150, article number 104835. doi: 10.1016/j.autcon.2023.104835.
[14] González-Herbón, R., González-Mateos, G., Rodríguez-Ossorio, J.R., Domínguez, M., Alonso, S., & Fuertes, J.J. (2024). An approach to develop digital twins in industry. *Sensors*, 24(3), article number 998. doi: 10.3390/s24030998.
[15] Hu, W., He, Y., Liu, Z., Tan, J., Yang, M., & Chen, J. (2021). Toward a digital twin: Time series prediction based on a hybrid ensemble empirical mode decomposition and BO-LSTM neural networks. *Journal of Mechanical Design*, 143(5), article number 051705. doi: 10.1115/1.4048414.
[16] IEC No. 62890:2020. (2020). *Industrial-process measurement, control and automation – life-cycle-management for systems and components*. Retrieved from https://webstore.iec.ch/en/publication/30583.
[17] ISO No. 23247-1. (2021). *Automation systems and integration – digital twin framework for manufacturing. Part 1: Overview and general principles*. Retrieved from https://www.iso.org/standard/75066.html.
[18] ISO No. 23247-2. (2021). *Automation systems and integration – digital twin framework for manufacturing. Part 2: Reference architecture*. Retrieved from https://www.iso.org/standard/78743.html.
[19] Javaid, M., Haleem, A., & Suman, R. (2023). Digital twin applications toward industry 4.0: A review. *Cognitive Robotics*, 3, 71-92. doi: 10.1016/j.cogr.2023.04.003.
[20] Jia, P., Wang, X., & Shen, X. (2022). Accurate and efficient digital twin construction using concurrent end-to-end synchronisation and multi-attribute data resampling. *IEEE Internet of Things Journal*, 10(6), 4857-4870. doi: 10.1109/JIOT.2022.3221012.
[21] Kamble, S.S., Gunasekaran, A., Parekh, H., Mani, V., Belhadi, A., & Sharma, R. (2022). Digital twin for sustainable manufacturing supply chains: Current trends, future perspectives, and an implementation framework. *Technological Forecasting and Social Change*, 176, article number 121448. doi: 10.1016/j.techfore.2021.121448.
[22] Kenett, R.S., & Bortman, J. (2022). The digital twin in Industry 4.0: A wide-angle perspective. *Quality and Reliability Engineering International*, 38(3), 1357-1366. doi: 10.1002/qre.2948.
[23] Khan, S., Arslan, T., & Ratnarajah, T. (2022). Digital twin perspective of fourth industrial and healthcare revolution. *IEEE Access*, 10, 25732-25754. doi: 10.1109/ACCESS.2022.3156062.
[24] Kuo, Y.H., Pilati, F., Qu, T., & Huang, G.Q. (2021). Digital twin-enabled smart industrial systems: Recent developments and future perspectives. *International Journal of Computer Integrated Manufacturing*, 34(7-8), 685-689. doi: 10.1080/0951192X.2021.1959710.
[25] Lee, J., Azamfar, M., Singh, J., & Siahpour, S. (2020). Integration of digital twin and deep learning in cyber-physical systems: Towards smart manufacturing. *IET Collaborative Intelligent Manufacturing*, 2(1), 34-36. doi: 10.1049/iet-cim.2020.0009.
[26] Liang, C.J., McGee, W., Menassa, C.C., & Kamat, V.R. (2022). Real-time state synchronisation between physical construction robots and process-level digital twins. *Construction Robotics*, 6, 57-73. doi: 10.1007/s41693-022-00068-1.
[27] Liu, Z., Meyendorf, N., Blasch, E., Tsukada, K., Liao, M., & Mrad, N. (2025). The role of data fusion in predictive maintenance using digital twins. In N. Meyendorf, N. Ida, R. Singh & J. Vrana (Eds.), *Handbook of nondestructive evaluation 4.0* (pp. 1-23). Cham: Springer. doi: 10.1007/978-3-030-48200-8_65-1.

[28] Lugaresi, G., Gangemi, S., Gazzoni, G., & Matta, A. (2023). Online validation of digital twins for manufacturing systems. *Computers in Industry*, 150, article number 103942. doi: 10.1016/j.compind.2023.103942.
[29] Ma, S., Ding, W., Liu, Y., Ren, S., & Yang, H. (2022). Digital twin and big data-driven sustainable smart manufacturing based on information management systems for energy-intensive industries. *Applied Energy*, 326, article number 119986. doi: 10.1016/j.apenergy.2022.119986.
[30] Melesse, T.Y., Di Pasquale, V., & Riemma, S. (2021). Digital Twin models in industrial operations: State-of-the-art and future research directions. *IET Collaborative Intelligent Manufacturing*, 3(1), 37-47. doi: 10.1049/cim2.12010.
[31] Moenck, K., Rath, J.E., Koch, J., Wendt, A., Kalscheuer, F., Schüppstuhl, T., & Schoepflin, D. (2024). Digital twins in aircraft production and MRO: Challenges and opportunities. *CEAS Aeronautical Journal*, 15, 1051-1067. doi: 10.1007/s13272-024-00740-y.
[32] Onaji, I., Tiwari, D., Soulatiantork, P., Song, B., & Tiwari, A. (2022). Digital twin in manufacturing: Conceptual framework and case studies. *International Journal of Computer Integrated Manufacturing*, 35(8), 831-858. doi: 10.1080/0951192X.2022.2027014.
[33] Plageras, A.P., & Psannis, K.E. (2022). Digital twins and multi-access edge computing for IIoT. *Virtual Reality & Intelligent Hardware*, 4(6), 521-534. doi: 10.1016/j.vrih.2022.07.005.
[34] Rovere, D., Pedrazzoli, P., dal Maso, G., Alge, M., & Ciavotta, M. (2022). A centralized support infrastructure (CSI) to manage CPS digital twin, towards the synchronisation between CPS deployed on the shopfloor and their digital representation. In J. Soldatos, O. Lazaro & F. Cavadini (Eds.), *The digital shopfloor – industrial automation in the Industry 4.0 era* (pp. 317-335). New York: River Publishers. doi: 10.1201/9781003339717.
[35] Savchuk, T., & Kozachuk, A. (2015). Automated decision-making for scaling a cloud application. *Information Technologies and Computer Engineering*, 12(2), 15-22.
[36] Siemens. (2023). *The 2022 digital twin report*. Retrieved from https://blogs.sw.siemens.com/wp-content/uploads/sites/41/2022/05/The-2022-Digital-Twin-Report-by-Lifecycle-Insights.pdf.
[37] Singh, M., Srivastava, R., Fuenmayor, E., Kuts, V., Qiao, Y., Murray, N., & Devine, D. (2022). Applications of digital twin across industries: A review. *Applied Sciences*, 12(11), article number 5727. doi: 10.3390/app12115727.
[38] Stergiou, C., & Psannis, K. (2022). Digital twin intelligent system for industrial internet of things-based big data management and analysis in cloud environments. *Virtual Reality & Intelligent Hardware*, 4(4), 279-291. doi: 10.1016/j.vrih.2022.05.003.
[39] Ucar, A., Karakose, M., & Kırımça, N. (2024). Artificial intelligence for predictive maintenance applications: Key components, trustworthiness, and future trends. *Applied Sciences*, 14(2), article number 898. doi: 10.3390/app14020898.
[40] Wang, Y., Fang, J., Cheng, Y., She, H., Guo, Y., & Zheng, G. (2023). Cooperative end-edge-cloud computing and resource allocation for digital twin enabled 6G industrial IoT. *IEEE Journal of Selected Topics in Signal Processing*, 18(1), 124-137. doi: 10.1109/JSTSP.2023.3345154.
[41] Yang, D., Karimi, H.R., Kaynak, O., & Yin, S. (2021). Developments of digital twin technologies in industrial, smart city and healthcare sectors: A survey. *Complex Engineering Systems*, 1, article number 3. doi: 10.20517/ces.2021.06.
[42] You, Y., Chen, C., Hu, F., Liu, Y., & Ji, Z. (2022). Advances of digital twins for predictive maintenance. *Procedia Computer Science*, 200, 1471-1480. doi: 10.1016/j.procs.2022.01.348.
[43] Yu, W., Patros, P., Young, B., Klinac, E., & Walmsley, T.G. (2022). Energy digital twin technology for industrial energy management: Classification, challenges and future. *Renewable and Sustainable Energy Reviews*, 161, article number 112407. doi: 10.1016/j.rser.2022.112407.
[44] Zhong, D., Xia, Z., Zhu, Y., & Duan, J. (2023). Overview of predictive maintenance based on digital twin technology. *Heliyon*, 9(4), article number e14534. doi: 10.1016/j.heliyon.2023.e14534.

Хмарні цифрові двійники: як симуляції можуть передбачати збої в промисловості

Віталій Ясененко

Магістр, старший розробник програмного забезпечення
TP-Link
92618, вул. Технологій Драйв, 36, м. Ірвайн, США
https://orcid.org/0009-0004-4801-9541

Анотація. Актуальність дослідження зумовлена зростанням складності промислових систем і необхідністю обробки великих потоків даних у реальному часі для забезпечення надійного моніторингу, прогнозування технічних збоїв і підтримки прийняття рішень. Метою роботи було ідентифікувати типові архітектурні конфігурації цифрових двійників у хмарному середовищі та визначити, як розподіл аналітичних функцій між архітектурними рівнями впливає на ефективність таких систем у виробничих умовах. Методологія дослідження ґрунтувалася на критичному аналізі міждисциплінарних джерел із застосуванням контент-аналізу, порівняльного аналізу та SWOT-аналізу, що дозволило здійснити тематичне структурування матеріалу за архітектурними, алгоритмічними та організаційно-нормативними параметрами. У результаті встановлено, що багаторівнева модель цифрового двійника є універсальною основою для опису архітектур у машинобудуванні, енергетиці й автоматизованому виробництві. Гібридні рішення з перенесенням частини аналітики на edge-рівень забезпечували підвищену стійкість до мережевих збоїв і кращу адаптацію до змін технічного стану об'єктів. Виявлено, що ефективність систем залежала не лише від топології обчислювальних задач, а й від здатності аналітичних моделей обробляти потокові дані, зберігати точність при дрейфі даних і залишатися інтерпретованими в умовах критичних рішень. Показано, що ключовими бар'єрами реалізації залишалися фрагментарність підходів до функціональної декомпозиції, відсутність єдиних стандартів та чутливість до нестабільної взаємодії між компонентами. На основі міжгалузевого зіставлення сформовано типологію архітектур цифрових двійників, що враховує характер розподілу аналітики та її інтеграцію з хмарною інфраструктурою. Отримані результати становлять концептуальну основу для подальших емпіричних досліджень, спрямованих на практичну верифікацію стабільності, адаптивності й масштабованості цифрових двійників у виробничих умовах

Ключові слова: потокова обробка даних; симуляційне прогнозування; виробничі IoT-системи; прогнозна аналітика; гібридна інфраструктура

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 11.04.2025
Revised: 22.08.2025
Accepted: 17.09.2025

UDC 621.3

DOI: 10.30857/2786-5371.2025.4.3

Research on methods for optimising the performance of VR applications in low-bandwidth browsers

Yan-Viktor Latyshev*

Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0000-6133-2736

Hanna Vlasiuk

Doctor of Technical Sciences, Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-7382-0435

Abstract. The relevance of the research lay in the need to improve the performance of WebVR applications in browser environments with limited network bandwidth, which is important for users with slow or unstable Internet connections. The aim of the work was to develop and evaluate effective methods that reduce scene loading times, optimise the amount of data transferred, and maintain a stable frame rate without compromising the quality of interaction. The study used experimental modelling of a virtual reality environment with limited network parameters. The work used open libraries for three-dimensional graphics with the ability to progressively load 3D resources. Several optimisation methods were implemented and compared, including multi-level model detailing, deferred loading, server-side geometry simplification, data compression, and texture decompression. The effectiveness was evaluated based on loading time, traffic volume, smoothness of playback, and system response. The results of the study showed that combining multi-level detailing with texture compression can reduce the amount of data transferred by up to 70% without noticeable loss of image quality. It was found that the use of progressive loading significantly reduces the initial scene rendering time, while client-side caching reduces repeat traffic by 90%. The most effective strategy was found to be the initial loading of simplified models with the subsequent asynchronous addition of detailed objects, which supports stable operation even at low Internet speeds. The practical value lies in the application of the developed methods in the creation of WebVR applications for education, medicine, commerce, and entertainment, especially in conditions of limited internet connection. This contributes to expanding the audience and reducing infrastructure costs

Keywords: WebXR; progressive loading; LOD; caching; texture compression; Three.js; A-Frame

Introduction

Modern virtual reality (VR) technologies are increasingly being integrated into the web environment thanks to the development of application programming interfaces (APIs) such as WebVR (Web Virtual Reality) and WebXR (Web Extended Reality). However, the performance of such solutions depends on the quality of the internet, which complicates access in regions with slow or unstable connections. Traditional VR applications that require the transfer of large amounts of 3D data are ineffective in such conditions. This necessitates the optimisation of VR content to take into account network limitations. The main task is to maintain a balance between visualisation quality and the amount of data transferred. Deterioration in quality reduces the user experience, while maintaining full detail complicates scene loading. This requires a comprehensive approach to optimisation, including the use of level-of-detail (LOD) models, resource compression, progressive loading, and efficient caching.

Globally, the current state of VR content optimisation for low-bandwidth web environments has been characterised by the active development of adaptive algorithms that take into account network fluctuations and limited resources. In particular, research focused on integrating WebXR

Suggested Citation:
Latyshev, Ya.-V., & Vlasiuk, H. (2025). Research on methods for optimising the performance of VR applications in low-bandwidth browsers. *Technologies and Engineering,* 26(4), 37-43. doi: 10.30857/2786-5371.2025.4.3.

*Corresponding author

with networks to reduce latency and optimise traffic. For example, H. Lee & Y. Hwang (2022) evaluated the use of VR technologies in web environments for educational purposes, emphasising the importance of an adaptive approach to resources and optimising interaction in conditions of limited bandwidth. F. Maura *et al*. (2024) worked on algorithms that automatically adjust the quality of VR video depending on network speed using Wi-Fi. Their research showed that such algorithms reduce video "freezing" by 20%, which is useful for creating smooth VR applications in browsers.

The research focused on streaming VR content in a web environment focused on user experience quality, where adaptive encoding, progressive loading, and caching methods were key. B. Fanini & G. Gosti (2024) developed a pipeline for immersive analytics based on WebXR, addressing network bottlenecks and performance issues in collaborative 3D environments, reducing data volume and latency in low-bandwidth conditions. J. Woo *et al.* (2024) proposed a method that predicts internet speed using artificial intelligence (Gated Recurrent Unit models) and adjusts video quality, reducing latency by 11% in mobile networks. This approach can be useful for adapting WebXR applications to low-speed conditions. B. Fanini *et al*. (2021) presented the ATON framework for creating immersive Web3D/WebXR applications, which adapts interfaces and rendering to devices, including resource optimisation for low-speed networks through compression and progressive loading.

B. Sobota *et al*. (2023) investigated the use of web-based 3D environments in primary and secondary education for children with multiple disabilities, demonstrating the practical applicability of such environments in conditions of limited technical resources and confirming the possibility of adapting content for poor network conditions. L. Franke & D. Haehn (2020) in their review of modern web visualisations emphasised the role of WebXR alongside the Web Graphics Library in optimising performance, allowing the creation of high-quality 3D experiences with less network load through efficient compression and caching. K.A. Mills *et al*. (2024) developed an approach to using VR games and multimodal 3D environments in education, which contributes to the effective optimisation of web VR content and improves the quality of interaction in educational systems. Overall, these works pointed to a trend towards using frameworks such as A-Frame and Three.js, machine learning, and edge computing to adapt VR content, but not enough attention has been paid to comprehensive optimisation for low-bandwidth browsers, especially in combination with LOD, progressive loading, and caching. For example, A.-M. Boutsi *et al.* (2023) emphasised the role of multi-resolution rendering schemes using the Three.js library and glTF formats with Draco compression to reduce the loading time of 3D models in networks with limited bandwidth. Similarly, a study by S.-M. Wang *et al*. (2022) described support for progressive asset loading and adaptive resource optimisation, which allows web VR applications to reduce the first render time on low-speed networks.

Scientific research in the field of WebVR is actively developing, but much of it is focused on high-speed connections or native VR environments. Insufficient attention is paid to the specifics of how VR applications function in browsers under unstable network conditions. The aim of the study was to develop effective optimisation strategies that minimise loading delays, reduce the amount of data transferred, and ensure a stable frame rate, while maintaining the quality of user interaction with the system even under conditions of limited computing resources.

Materials and Methods

The study focused on optimising WebVR applications for browsers under low network bandwidth conditions (less than 2 Mbit/s). The methodology was developed to ensure a stable frame rate of 60 frames per second (FPS), reduce loading delays, and maintain the quality of the user experience. The study used data from S. Pacheco-Gutierrez *et al*. (2021), Three.js (n.d.), and A-Frame Documentation (n.d.). A WebVR/WebXR test scene was created using the Three.js and A-Frame libraries. The scene contained 3D models (up to 120,000 polygons), physically correct textures, dynamic lighting, and animation that simulated typical VR applications. Testing was conducted at a network speed of 1-2 Mbit/s, reflecting real conditions in regions with slow internet.

Three methods were tested: dynamic level-of-detail (LOD) replacement, texture compression in .basis format, and progressive loading with caching via Service Workers. The experiments were conducted on laptops (Intel UHD Graphics) and smartphones (Android/iOS) in Chrome, Firefox, and Edge browsers with WebXR support. The glTF models had simplified (3-5 thousand polygons) and detailed (up to 100 thousand) versions. .basis textures were selected based on network speed via navigator.connection.downlink. The scene was created with LOD, textures were compressed with the Basis Universal tool, and Service Workers cached the data. Performance was evaluated based on loading time (performance.now()), FPS, data volume, and graphics processing unit (GPU) load, measured using Chrome DevTools. The sample included several scenarios, each with 5-15 objects, to evaluate the methods under different conditions. Table 1 summarises the data for each scenario. The methodology allowed to test the effectiveness of the combination of LOD, texture compression, progressive loading, and caching under low bandwidth conditions. The choice of methods was justified by their proven effectiveness in other studies (Pacheco-Gutierrez *et al*., 2021; Žádník *et al*., 2022; Liu *et al*., 2023).

Table 1. *Description of test scenarios*

Scenario	Number of objects	Content type	Main parameters
Scenario 1	5	Static objects	Simplified models, 512 x 512 textures
Scenario 2	8	Mixed	Detailed models, 1024 x 1024 textures

Table 1. Continued

Scenario	Number of objects	Content type	Main parameters
Scenario 3	12	Dynamic objects	Animation, 2048 x 2048 textures
Scenario 4	15	Complex scene	LOD, .basis compression, delta updates

Source: *developed by the authors based on experimental data*

These approaches were implemented in detail to assess their effectiveness in practical conditions. In particular, dynamic LOD replacement involved loading two versions of models – simplified (3-5 thousand polygons) and detailed (up to 100 thousand polygons). Simplified models were loaded first, and detailed models were loaded asynchronously after scene initialisation. Formally, this approach is described as two-phase scene initialisation:

$$T_{total} = T_{init}^{low} + T_{defer}^{high}, \quad (1)$$

where T_{init}^{low} – initialisation time for simplified models, and, T_{defer}^{high} – asynchronous loading of detailed models.

Additionally, a method of adaptive texture replacement using the .basis format has been implemented. Several texture options (512 x 512, 1024 x 1024, 2048 x 2048) have been prepared for each object. The principle was calculated using the formula:

$$T = \frac{S * 8}{B}, \quad (2)$$

where S – size of transmitted data, B – network bandwidth.

For example, for S = 3 MB and B = 1 Mbit/s, T was 24 seconds. When using Basis Universal, the size was reduced to 0.6 MB, which corresponded to only 4.8 seconds. To reduce the load on the GPU, simplified 256 x 256 normal maps were used to simulate a complex surface (according to Chrome DevTools). Shaders (graphics processing programs) were also optimised: instead of complex mathematical effects, simple textures were used, the number of light sources was limited to two, and materials were changed to less resource-intensive ones (MeshStandardMaterial instead of MeshPhysicalMaterial). The optimised loading code is shown in Figure 1.

```
const modelLow = await loadGLTF('models/scene_low.glb')
scene.add(modelLow)

initScene().then(() => {
  loadGLTFAsync('models/scene_high.glb').then(modelHigh => {
    scene.remove(modelLow)
    scene.add(modelHigh)
  })
})
```

Figure 1*. Optimised loading code*
Source: *developed by the authors based on data from Three.js (n.d.), A-Frame Documentation (n.d.)*

The "delta change transmission" method was considered separately – instead of a complete scene update, only changes in the positions, rotations and states of objects are transmitted. For example, instead of JavaScript Object Notation (JSON) with a full description of 1,000 objects (~2 MB), only ID arrays and change vectors were transmitted, which reduced the average payload size to 40-60 KB per frame (Fig. 2).

```
[
  {"id": "chair_2", "position": [1.2, 0, 3.3], "rotation": [0, 90, 0]},
  {"id": "door_1", "open": true}
]
```

Figure 2*. Structure of the delta package for updating scene objects in JSON format*
Source: *developed by the authors based on materials from S. Pacheco-Gutierrez et al. (2021)*

Thus, the developed methodology provided a comprehensive verification of the impact of key WebVR application optimisation techniques in low-bandwidth browsers. It combined LOD levels, adaptive texture compression, and caching mechanisms, allowing to evaluate not only individual performance parameters but also system stability during dynamic scene updates. The methodology was reproducible because it uses open-source tools Three.js and A-Frame.

Results and Discussion

Initial tests showed that loading full-size models and textures with a resolution of 2048x2048 at a speed of 1 Mbit/s resulted in a first render time of 12.4 seconds and a frame rate of no more than 24 FPS. Testing was conducted across four scenarios covering static, mixed, dynamic, and complex scenes. A comparison of methods showed that LOD with deferred loading of detailed models provided the fastest initial rendering. Texture compression provided the greatest reduction in latency, although low-quality textures slightly reduced visual quality. Delta updates were most effective for dynamic scenes, transmitting only 2-3% of the data from the full scene state with an update time of less than 100 ms. The combination of all methods allowed to achieve a stable 60 FPS on devices with a weak graphics core (Intel UHD) at speeds of less than 1 Mbit/s (scenario 4). Key metrics: reduction in GPU frame time from 48 ms to 15 ms, first render time from 9.6 s to 2.8 s, data volume from 24 MB to 3.1 MB (Table 2).

Table 2. *Comparison of optimisation method performance*

Method	First render time (s)	FPS	Data volume (MB)	GPU frame time (ms)
Without optimisation	12.4 ± 0.5	24	24.0 ± 1.0	48 ± 2
LOD	4.2 ± 0.2	57-60	6.5 ± 0.3	20 ± 1
Compression .basis	5.1 ± 0.3	55-60	3.1 ± 0.2	18 ± 1
Delta updates	6.8 ± 0.4	58-60	4.0 ± 0.2	17 ± 1
Combination of methods	2.8 ± 0.2	60	3.1 ± 0.2	15 ± 1

Source: *developed by the authors based on experimental data*

The results showed that each optimisation method has its advantages depending on the type of content. In particular, the use of LOD proved to be most effective for static scenes with a large amount of geometry (scenario 1), as it allows simplified models to be displayed quickly and detailed ones to be loaded gradually. LOD reduced the time to first render to 4.2 ± 0.2 seconds, providing a stable 57-60 FPS even on devices with basic graphics. Texture compression in .basis format is best suited for projects with a large amount of graphic material (scenario 2), providing a significant reduction in loading time without noticeable loss of quality. The amount of data transferred was reduced to 3.1 ± 0.2 MB, which gave the best results on slow networks. Delta updates showed the best results for dynamic scenes with a large number of moving objects (scenario 3), as they only transmit changes in states, reducing traffic several times over. Delta updates minimised scene update latency, delivering a stable 58-60 FPS even in dynamic scenarios. The combined use of all methods ensures versatility and stable performance regardless of scene complexity or network speed.

A detailed review of the results showed that the LOD method was most beneficial in cases where fast first rendering was key. Scene appearance time was reduced by more than three times compared to the baseline, and the reduction in GPU load allowed for consistently high FPS even on devices with limited resources. This was particularly noticeable on laptops with Intel UHD, where performance improved the most. The only exception was Firefox, where short drops sometimes occurred during the gradual loading of details, but they did not have a critical impact on the user experience. The results for compressing textures in .basis format were different. Its main advantage was the maximum reduction in the amount of data transferred, which resulted in a significant gain in bandwidth. This effect is especially important in slow networks, where .basis made it possible to avoid long delays and maintain smooth scene rendering. At the same time, performance varied slightly depending on the platform: on iOS, hardware support accelerated decompression, while on Android, with less powerful hardware, additional delays were observed. This indicated that the effectiveness of the method is highly dependent on the specific execution environment.

Delta updates had the greatest impact on reducing network traffic. The amount of data transferred was reduced tenfold, which had a positive effect on the interactivity of dynamic scenes. As a result, the system's response time approached real time, and the frame rate remained virtually unchanged. On mobile devices, the mechanism worked flawlessly in Chrome and Edge, while in Firefox there were cases of request accumulation, which caused short pauses in the update. Despite this, the average performance remained within a comfortable range of 58-60 FPS. Comparing the methods according to key metrics (Table 2) reveals a clear distribution of strengths: LOD provided the best optimisation of start-up time, .basis offers the most effective reduction in network traffic, and delta updates reduce GPU load while ensuring high system responsiveness. The combined use of these techniques allowed to combine their advantages: rendering started in less than three seconds, data volumes were reduced by almost eight times, and the load on the GPU fell threefold compared to the initial conditions.

Analysis of results on different devices confirmed the versatility of the combined approach. On laptops with integrated graphics, performance reached a stable 60 FPS even at network speeds below 1 Mbps. Android smartphones showed slightly higher latency due to slower decompression, but the average frame rate did not drop below 55 FPS. iOS devices proved to be the most stable thanks to hardware optimisation, making them the most convenient platform for applying such techniques. Thus, all three methods have different effects on key metrics, but their combination provides the most balanced result for different types of scenes and different technical conditions. This ensures an acceptable quality of experience even on low-bandwidth networks and devices with weak graphics cores.

A comparison with other studies revealed similarities in approaches, but also revealed important differences. For example, A.-M. Boutsi *et al*. (2023) achieved a 46% reduction in render time using multi-resolution 3D rendering, which is similar to the author's LOD, but their methodology was not focused on low-bandwidth scenarios (tests were conducted mainly at speeds >5 Mbit/s). In contrast, the approach in this article showed stable 57-60 FPS even at <2 Mbit/s, making it suitable for a wider range of use cases. B. Fanini *et al*. (2021) reduced the data volume by 50% in WebXR using the ATON framework, which is partially consistent with the authors' results (73% for LOD), but the lack of integration with texture compression limited the overall effect. In the current work, the combination of methods yielded a more balanced result: a reduction in render time to 2.8 s while reducing the data volume by more than seven times. A similar optimisation effect was demonstrated by J. Wang *et al*. (2022), who implemented direct training of a voxel feature grid for high-precision surface reconstruction from RGB-D sequences in the GO-Surf project. Their method combines local geometric and visual features in a multi-level structure and provides

fast reconstruction with minimal deviation between synthesised and real data without the need for post-processing.

M. De Fré *et al*. (2024) showed that optimisation through caching can reduce the number of server requests by 70%, which is consistent with the authors' results, but their research focused primarily on video conferencing. The current results for VR content showed even greater relevance of this approach in interactive environments, where repeated requests significantly affect the user experience. M. Lim *et al*. (2025) achieved a 30% reduction in latency at speeds of 2-4 Mbit/s in the WIDE-VR project, but their system was optimised for a wider range of network conditions. In contrast, this study showed that under narrow constraints (<2 Mbit/s), the efficiency can be even higher: FPS increased from 24 to 60, and response time was reduced by more than half, making the approach more relevant for weak network environments. Similar results in terms of latency reduction were confirmed by S. Uddin *et al*. (2025), who investigated the effectiveness of low-latency adaptive bitrate algorithms within the framework of Hypertext Transfer Protocol adaptive streaming and showed that such algorithms provide a consistently high quality user experience even with fluctuations in network bandwidth.

Similar parallels can be found in the work of I. Yeregui *et al*. (2025), who investigated the optimisation of VR environments in the context of 5G networks. Although their results demonstrated a high level of adaptation and reduced latency thanks to network infrastructure, the authors of the current study focused on a more universal scenario – browser limitations, where 5G is not always available. This revealed a difference in areas of application: their approach is geared towards technologically advanced environments, while the authors' approach has practical value even in countries with lower quality network services. According to the results of W.J. Kim & B.B. Khomtchouk (2024), processing was accelerated by 63% thanks to WebAssembly. Although their work did not cover LOD or texture compression, it demonstrated the promise of combined technologies. The current results showed that combining traditional optimisations with modern tools such as WebAssembly or WebGPU can provide even better results, which is consistent with the system optimisation approach proposed by D. Honcharenko *et al*. (2023), who used multi-criteria analysis to select optimal technologies in IoT systems for monitoring physical indicators. In this sense, the authors' approach laid the foundation for future research, where classical methods will be integrated with new web technology standards.

It is also important to note the results of the study by C. Slocum *et al*. (2021), who presented the VIA system with selective loading of only those 3D objects that are in the user's field of view. This made it possible to reduce the scene rendering time by 50% at speeds of about 10 Mbit/s. However, this approach proved to be less effective in low-bandwidth scenarios, where the load remains significant even with partial model loading. The authors' research showed that a combination of LOD, delta updates, and texture compression allows for greater flexibility. This indicates that the proposed approach can be effective in a wider range of network conditions and be more resistant to extreme constraints than traditional visibility methods.

Thus, the authors' combined approach not only surpasses individual solutions in terms of versatility, but also demonstrates better adaptability to low-bandwidth conditions. This has been confirmed by direct comparisons with previous works: while other researchers have mostly tested systems in environments with medium or high network speeds, the current study has shown that even under minimal conditions (<2 Mbit/s), a significant performance improvement can be achieved without compromising the quality of the user experience.

Conclusions

The study evaluated methods for optimising WebVR applications for browsers under low bandwidth conditions (less than 2 Mbit/s). Experiments using the Three.js and A-Frame libraries confirmed that a combination of dynamic LOD replacement, texture compression in .basis format, and delta updates with caching via Service Workers significantly improves performance. The first render time was reduced from 12.4 to 2.8 seconds, the amount of data transferred was reduced from 24 MB to 3.1 MB, and the frame rate stabilised at 60 FPS on devices with a weak graphics core (Intel UHD) at network speeds of less than 1 Mbit/s. The use of LOD with initial loading of simplified models (3-5 thousand polygons) and asynchronous addition of detailed ones (up to 100 thousand polygons) ensured fast initial rendering. Compression of .basis textures reduced their size by 6-8 times, which reduced loading delays by 80%, as shown by measurements using performance.now.() Delta updates reduced the amount of data to 40-60 KB per frame, which proved to be effective for dynamic scenes. The combination of these methods outperformed individual approaches, ensuring stable performance. Additionally, analysis of the results showed that the combined approach allowed maintaining a stable frame rate even when the number of objects in the scene was increased to 15, confirming its scalability. It was also found that the use of simplified 256 x 256 pixel normal maps reduced peak GPU loads by 30%, and optimising shaders by limiting light sources to two reduced graphics processing time by 20% compared to the initial settings. Prospects for further research include integrating machine learning to predict network conditions and using WebGPU to accelerate graphics processing in browsers, which could further reduce latency and improve rendering quality.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] A-Frame Documentation. (n.d.). *Asset management system*. Retrieved from https://aframe.io/docs/1.7.0/core/asset-management-system.html.

[2] Boutsi, A.-M., Ioannidis, C., & Verykokou, S. (2023). Multi-resolution 3D rendering for high-performance web AR. *Sensors*, 23(15), article number 6885. doi: 10.3390/s23156885.

[3] De Fré, M., van der Hooft, J., Wauters, T., & De Turck, F. (2024). Demonstrating adaptive many-to-many immersive teleconferencing for volumetric video. In *Proceedings of the 15th ACM multimedia systems conference* (pp. 453-458). New York: Association for Computing Machinery. doi: 10.1145/3625468.3652192.

[4] Fanini, B., & Gosti, G. (2024). A new generation of collaborative immersive analytics on the web: Open-source services to capture, process and inspect users' sessions in 3D environments. *Future Internet*, 16(5), article number 147. doi: 10.3390/fi16050147.

[5] Fanini, B., Ferdani, D., Demetrescu, E., Berto, S., & d'Annibale, E. (2021). ATON: An open-source framework for creating immersive, collaborative and liquid web-appsfor cultural heritage. *Applied Sciences*, 11(22), article number 11062. doi: 10.3390/app112211062.

[6] Franke, L., & Haehn, D. (2020). Modern scientific visualizations on the web. *Informatics*, 7(4), article number 37. doi: 10.3390/informatics7040037.

[7] Honcharenko, D., Mokin, V., & Protsenko, D. (2023). Building an information system for monitoring physical indicators based on the Internet of Things technology. *Information Technologies and Computer Engineering*, 20(2), 99-108. doi: 10.31649/1999-9941-2023-57-2-99-108.

[8] Mills, K.A., Brown, A., & Funnell, P. (2024). Virtual reality games for 3D multimodal designing and knowledge across the curriculum. *The Australian Educational Researcher*, 51, 2323-2353. doi: 10.1007/s13384-024-00695-3.

[9] Kim, W.J., & Khomtchouk, B.B. (2024). WebAssembly enables low latency interoperable augmented and virtual reality software. *arXiv*. doi: 10.48550/arXiv.2110.07128.

[10] Sobota, B., Korečko, Š., & Mattová, M. (2023). Web-based 3D virtual environments utilization in primary and secondary education of children with multiple impairments. *Electronics*, 12(13), article number 2792. doi: 10.3390/electronics12132792.

[11] Lee, H., & Hwang, Y. (2022). Technology-enhanced education through VR-making and metaverse-linking to foster teacher readiness and sustainable learning. *Sustainability*, 14(8), article number 4786. doi: 10.3390/su14084786.

[12] Lim, M., Bentaleb, A., & Zimmermann, R. (2025). WIDE-VR: An open-source prototype for web-based VR through adaptive streaming of 6DoF content and viewport prediction. In *Proceedings of the 16th ACM multimedia systems conference* (pp. 221-227). New York: Association for Computing Machinery. doi: 10.1145/3712676.3718334.

[13] Liu, K., Wu, N., & Han, B. (2023). Demystifying web-based mobile extended reality accelerated by WebGPU. In *Proceedings of the 2023 ACM on internet measurement conference* (pp. 145-153). New York: Association for Computing Machinery. doi: 10.1145/3618257.3624833.

[14] Maura, F., Casasnovas, M., & Bellalta, B. (2024). Experimenting with adaptive bitrate algorithms for virtual reality streaming over Wi-Fi. *arXiv*. doi: 10.48550/arXiv.2407.15614.

[15] Pacheco-Gutierrez, S., Niu, H., Caliskanelli, I., & Skilton, R. (2021). A multiple level-of-detail 3D data transmission approach for low-latency remote visualisation in teleoperation tasks. *Robotics*, 10(3), article number 89. doi: 10.3390/robotics10030089.

[16] Slocum, C., Huang, J., & Chen, J. (2021). VIA: Visibility-aware web-based virtual reality. In *Proceedings of the 26th international conference on 3D web technology* (article number 7). New York: Association for Computing Machinery. doi: 10.1145/3485444.3487641.

[17] Three.js. (n.d.). *DRACOLoader: A loader for geometry compressed with the Draco library*. Retrieved from https://threejs.org/docs/#examples/en/loaders/DRACOLoader.

[18] Uddin, S., Grega, M., Leszczuk, M., & ur Rahman, W. (2025). Evaluating HAS and low-latency streaming algorithms for enhanced QoE. *Electronics*, 14(13), article number 2587. doi: 10.3390/electronics14132587.

[19] Wang, J., Bleja, T., & Agapito, L. (2022). GO-Surf: Neural feature grid optimization for fast, high-fidelity RGB-D surface reconstruction. *arXiv*. doi: 10.48550/arXiv.2206.14735.

[20] Wang., S.-M., Yaqin, M.A., & Hsu, F.-H. (2022). AHP-based assessment of developing online virtual reality services with progressive web apps. *EasyChair Preprint*, 9501, 1-12.

[21] Woo, J., Hong, S., Kang, D., & An, D. (2024). Improving the quality of experience of video streaming through a buffer-based adaptive bitrate algorithm and gated recurrent unit-based network bandwidth prediction. *Applied Sciences*, 14(22), article number 10490. doi: 10.3390/app142210490.

[22] Yeregui, I., Mejías, D., Zorrilla, M., Viola, R., Astorga, J., & Jacob, E. (2025). Leveraging 5G physical layer monitoring for adaptive remote rendering in XR applications. *arXiv*. doi: 10.48550/arXiv.2505.22123.

[23] Žádník, J., Mäkitalo, M., Vanne, J., & Jääskeläinen, P. (2022). Image and video coding techniques for ultra-low latency. *ACM Computing Surveys (CSUR)*, 54(11), article number 231. doi: 10.1145/3512342.

Дослідження засобів оптимізації продуктивності VR-додатків у браузерах з низькою пропускною здатністю

Ян-Віктор Латишев

Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0009-0000-6133-2736

Ганна Власюк

Доктор технічних наук, професор
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-7382-0435

Анотація. Актуальність дослідження полягала у необхідності підвищення продуктивності WebVR-додатків у браузерних середовищах за умов обмеженої пропускної здатності мережі, що є важливим для користувачів із повільним або нестабільним інтернет-з'єднанням. Метою роботи була розробка і оцінка ефективних методів, які дозволяють зменшити час завантаження сцен, оптимізувати обсяг передаваних даних та підтримувати стабільну частоту кадрів без зниження якості взаємодії. Для дослідження застосовано експериментальне моделювання середовища віртуальної реальності із використанням обмежених параметрів мережі. В роботі використано відкриті бібліотеки для тривимірної графіки з можливістю прогресивного завантаження 3D-ресурсів. Реалізовано та порівняно декілька методів оптимізації, зокрема багаторівневе деталювання моделей, відкладене завантаження, спрощення геометрії на сервері, компресію даних і декомпресію текстур. Оцінювання ефективності проводилось за показниками часу завантаження, обсягу переданого трафіку, плавності відтворення та відгуку системи. Результати дослідження продемонстрували, що поєднання багаторівневого деталювання з стисненням текстур дозволяє скоротити обсяг переданих даних до 70 % без помітної втрати якості зображення. Виявлено, що використання прогресивного завантаження значно знижує час первинного відображення сцени, кешування на боці клієнта зменшує повторний трафік на 90 %. Найефективнішою виявилася стратегія початкового завантаження спрощених моделей з подальшим асинхронним додаванням детальних об'єктів, що підтримує стабільну роботу навіть за низької швидкості інтернету. Практична цінність полягає у застосуванні розроблених методів при створенні WebVR-додатків для освіти, медицини, торгівлі та розваг, особливо в умовах обмеженого інтернет-з'єднання. Це сприяє розширенню аудиторії та зниженню витрат на інфраструктуру

Ключові слова: WebXR; прогресивне завантаження; LOD; кешування; стиснення текстур; Three.js; A-Frame

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 02.05.2025
Revised: 25.08.2025
Accepted: 17.09.2025

UDC 678

DOI: 10.30857/2786-5371.2025.4.4

Development of microtextures on polymer surfaces using the transfer method from metal templates

Oleksiy Myronyuk
Doctor of Technical Sciences, Associate Professor
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteyskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-0499-9491
Denys Baklan
PhD
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteyskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-6608-0117
Anna Bilousova*
Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteyskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-2818-8450
Volodymyr Strashenko
Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteyskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0009-3601-1821

Abstract. Scaling up technologies for creating relief surfaces with controlled wetting properties is a pressing issue for the development of functional polymer materials. There is a need to investigate the patterns of transfer of micro- and nanotextures from metal templates to polymer substrates. The purpose of the study was to determine the influence of the replication method and polymer properties on the accuracy of relief reproduction and the development of water-repellent surface characteristics. Three replication methods were used for this purpose: obtaining polycarbonate film from a solution, reaction moulding using polydimethylsiloxane elastomer, and thermoforming of polyethylene films. The negative copies obtained were used as intermediate forms (polycarbonate) for creating positive replicas from polyethylene and polysiloxane. The hydrophobicity of the materials was evaluated by measuring the contact angles in directions parallel and perpendicular to the texture orientation. The results showed that all methods ensure the reproduction of periodic structures. However, the level of accuracy depends on the viscosity of the medium and the temperature conditions, with the lowest level of accuracy observed for polycarbonate and the highest level observed for polyethylene. Polycarbonate negatives were characterised by high detail of microdefects (up to 5 μm), while polyethylene films showed smoothing of the relief. Silicone positives most fully preserved the geometry of the original textures with defects. The study of surface hydrophobicity showed a significant increase in contact angles on structured surfaces compared to smooth ones, especially with parallel orientation. The maximum contact angles reached 140°C for polysiloxane and 139°C for polyethylene replicas of the structure with regular grooves. The practical significance of the study lay in identifying the optimal materials and methods for creating polymer surfaces with increased water repellency. Polycarbonate is suitable for use as an intermediate material for accurate texture copying, while silicone and polyethylene have potential for use as functional surfaces in protective coatings and liquid-infused porous surfaces

Keywords: contact angle; polycarbonate; silicone; polyethylene; hydrophobicity

Suggested Citation:
Myronyuk, O., Baklan, D., Bilousova, A., & Strashenko, V. (2025). Development of microtextures on polymer surfaces using the transfer method from metal templates. *Technologies and Engineering,* 26(4), 44-53. doi: 10.30857/2786-5371.2025.4.4.

*Corresponding author

Introduction

Liquid-infused porous surfaces (LIPS) combine a porous or textured substrate with a lubricating liquid, enabling stable repellent behaviour in conditions where conventional superhydrophobic coatings prove unreliable. Such surfaces have found application in areas such as corrosion protection and anti-icing. It is the combination of stability under dynamic impact, resistance to condensation, and layer renewability that makes these surfaces a promising technology for large-scale solutions. Y. Meng *et al*. (2025) reviewed that LIPS materials represent an advancement of previously known textured surfaces which, upon reaching a Cassie state, could exhibit superhydrophobicity – characterised by water contact angles exceeding 150°. I.W. Park *et al*. (2023) reviewed that LIPS properties such as self-cleaning, water repellency, and resistance to ice formation are ensured by the Cassie-Baxter wetting state, which is achieved by high surface roughness and low surface energy of the material itself.

G. McHale *et al.* (2023) characterised significant drawbacks that served as fundamental limitations to practical application of LIPS. A limited range of liquid surface tensions was exhibited with which they could effectively repel. When the surface tension of a liquid dropped below this threshold, a transition occurred from the Cassie-Baxter state to the Wenzel state. H. Xie & H. Huang (2020) described this transition as a result in partial surface wetting, with liquid penetrating and being retained within the texture grooves – an effect directly opposite to the intended purpose of such surfaces for liquid repellency. In addition, D. Tripathi *et al*. (2023) found that LIPS are dynamically unstable. Specifically, when a droplet of wetting liquid hit them at a certain speed, it could change the state from Cassie-Baxter to Wenzel. Additionally, such surfaces were unstable against water vapour condensation. S. Adera *et al*. (2021) showed that in humid atmospheres, the enhanced water-repellent properties associated with superhydrophobicity diminished over time.

S. Peppou-Chapman *et al.* (2020) reviewed drawbacks of LIPS. Their water-repellent performance is lower than that of superhydrophobic surfaces because the infusion liquid's polarity is higher than air's. They are more stable than other surfaces, however, this is conditioned by their lack of open cavities that could be filled by water. Q. Cai *et al.* (2023) described that LIPS fabrication technologies are similar to those for superhydrophobic surfaces. They rely on the same methods to produce the structural layer that retains the infusion liquid. Sponges, electrospun surfaces, nonwoven materials, and porous substrates can be used as porous media. I.N. Etim *et al*. (2025) researched LIPS fabrication methods. These methods have the same drawback as for superhydrophobic surfaces: their widespread adoption and practical implementation are significantly limited by the inherently low scalability of the available fabrication techniques. P. Gao *et al*. (2023) showed that texture transfer by injection moulding of polypropylene and polymethyl methacrylate is a promising method for obtaining textured materials that are wettable according to the Cassie-Baxter state. The proposed method is inexpensive and easily scalable, although obtaining a shape with the required hierarchical structure has low productivity and high cost due to laser processing.

Challenges may arise during the texture transfer from metallic substrates to polyethylene and subsequently to polydimethylsiloxane, particularly regarding the loss of original structural features. This investigation focused on transfer fidelity and geometric discrepancies between successive replicas. Thus, the primary objective of this study was to investigate the regularities governing texture transfer from metallic templates onto polyethylene and polydimethylsiloxane (PDMS) substrates, using thermocompression, solution castings, and reactive moulding techniques, respectively.

Materials and Methods

The present study addressed the fabrication of scalable liquid-retaining structural layers using thermoforming and reactive curing techniques. Polyethylene was selected for thermocompression due to its low polarity, cost, and availability, while PDMS served as a reactive material capable of accurately reproducing surface textures. Stainless steel (AISI 304) plates textured by femtosecond laser were used as primary moulds, creating microstructures with features up to 10 μm and groove depths of 20-30 μm. Such laser texturing can also generate secondary periodic features that influence polymer melt and interfacial adhesion, an effect further examined in this study.

Although laser texturing created well-defined protrusions, the bottom of the grooves often formed unpredictable conical depressions that appeared as unwanted protrusions on the reproduced polymer surfaces (Bonse *et al*., 2021). To minimise these artefacts, an intermediate replica layer was introduced between the metal template and polyethylene. Polycarbonate was chosen for this purpose due to its high melting point, good mouldability, and ease of dissolution in common solvents. Its low adhesion to metal surfaces (Du *et al*., 2023) also facilitated defect-free separation of moulded films.

The basic textures on the surface of steel were obtained by femtosecond laser ablations described in previous paper (Myronyuk *et al*., 2023) with parameters shown in Table 1. This study was designed to investigate the relationship between the quality of microtexture transfer from metal templates to polymer materials. The quality of microtexture geometry replication on the surface, compared replication techniques, and compared the wettability of the resulting textured surfaces were evaluated. The study employed a combination of experimental and analytical methods, including replication via solution casting, reactive moulding, and thermal embossing. This was followed by microscopic characterisation and contact angle analysis. The overall methodology was based on a comparative evaluation of textured samples obtained using different replication methods while maintaining substrate topographies.

***Table 1**. Parameters of the texture grooves*

Texture	Material	Type	Groove width, μm	Groove depth, μm	Texture period, μm
A	AlSI304	positive	24.8 ± 2	19.5 ± 1	60 ± 2
B	AlSI304	positive	40 ± 1	24.5 ± 2	60 ± 1

***Source:** O. Myronyuk et al. (2023)*

In this study, three methods were employed to replicate textures from metallic templates:

1) A solution-based approach involved the use of a 5 wt. % dichloromethane solution of polycarbonate Calibre 303 10 TNT (Dow Chemicals). This solution was cast onto the surface of the textured metallic plate and left at room temperature for 1 h. to allow dichloromethane evaporation. To ensure complete removal of residual solvent, the samples were subsequently placed in a drying oven at 80°C for an additional 3 h. The resulting films were detached from the metallic templates due to shrinkage during solvent evaporation.

2) Reactive moulding method was performed using a polydimethylsiloxane elastomer. A two-component, platinum-catalysed, addition-curing PDMS system (SKA 035man. Silikony SK, Slovak Republic) was employed. After mixing, the liquid reactive composition was poured onto the surface of the textured sample, with the edges confined by a polyethylene ring. The assembly was then subjected to vacuum treatment to remove entrapped air. Following this step, the specimen was left to cure for 3 days, after which the silicone negative was carefully detached from the metallic plate.

3) A thermal moulding method (thermo-pressing) was performed by heating of metallic templates using a magnetic stirrer heater (RIVA-03.6, UOSLAB, Ukraine) to approximately 115°C. A low-density polyethylene film was then placed onto the heated surface and rolled with a polyurethane roller to ensure complete imprinting of the structure. Following this step, the template was carefully removed from the plate, allowed to cool to room temperature, and the textured polyethylene layer was mechanically detached.

The textures obtained by these methods were referred to as negative, as they represented inverse replicas of the original positive textures present on the metallic templates. To obtain positive replicas – specifically from polydimethylsiloxane, polyethylene, and polycarbonate – the polycarbonate negative was employed as the intermediate template. In this approach, thermoforming with polyethylene was carried out not on the metallic plate but on the polycarbonate negative, taking advantage of the fact that the melting temperature of polycarbonate is significantly higher than that of polyethylene. A similar procedure was applied during reactive curing: the PDMS mixture was cast onto the surface of the polycarbonate negative and left to cure under the same conditions as those used with the metallic template. To obtain a polycarbonate positive, the same polycarbonate solution described earlier was employed. However, instead of casting onto the metallic template, the solution was applied onto a PDMS negative, which served as the replication substrate.

The water contact angle was measured using the combination of Konus Academy 2 (Italy) optical microscope with goniometric setup and digital camera UCMOS 1300 (Sigeta) images were processed using the ToupView software (ToupTek). The same complex was used for obtaining the optical microscopy images of the microtextured surfaces. In this study, extended textures oriented along a single axis were employed. Of particular interest was the evaluation of wetting behaviour in two orthogonal directions, namely parallel and perpendicular to the texture orientation. Accordingly, throughout this study these areas were referred to as the parallel and perpendicular orientations, as schematically illustrated in Figure 1. Deionised water and dichloromethane (solvent for polycarbonate) were used as supplementary materials in this study.

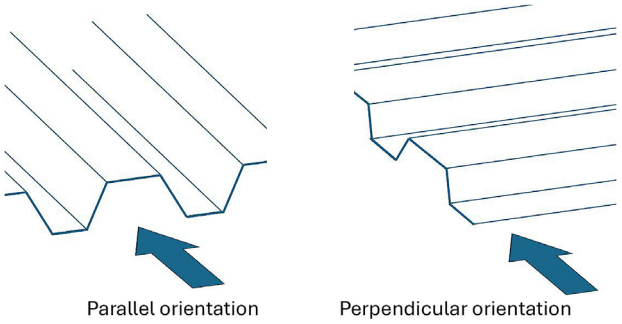

***Figure 1**. Water contact angle measurement directions*
***Source:** developed by the authors of this study*

Overall, the experimental procedure involved several sequential stages: (1) generation of primary laser-induced textures on steel templates; (2) replication of these textures into polymeric negative; (3) fabrication of positive polysiloxane and polyethylene replicas through moulding; and (4) characterisation of surface morphology and wetting behaviour in orthogonal directions. This structure ensured a consistent framework for comparing replication accuracy and material-specific behaviour under identical texturing conditions. Such an approach allowed for a comprehensive methodological assessment of the efficiency and reproducibility of polymer texture transfer processes.

Results and Discussion

The textures that were used as metal templates (Fig. 2) have a linear grooves pattern divided with asperities. For the texture A, the period is well-reproduced 60 μm with the groove width 25 μm. The asperity has a larger width – 35 μm. In the case of this structure, the grooves have the profile of a reverse triangle with the height of 19 μm. Even in optical microscopy photos it is seen that the sides of these

triangles are irregular due to the uneven removal of the material during the laser ablation. The texture B has the same period – 60 μm, but a significantly wider groove that is 45 μm with the asperity width 15 μm. It is seen that the groove in this case has the inverse trapezoid profile with small diameter holes on the bottom. These holes may be seen in both A and B textures and are typically formed at the places of the laser beam focusing. Thus, as evident from the texture images, the groove surfaces appear highly heterogeneous. They exhibit distinct artefacts and localised accumulations of material. Moreover, closer inspection reveals that the ridges themselves are far from perfectly smooth. Together, these two factors pose significant challenges when attempting to replicate such surfaces with high fidelity.

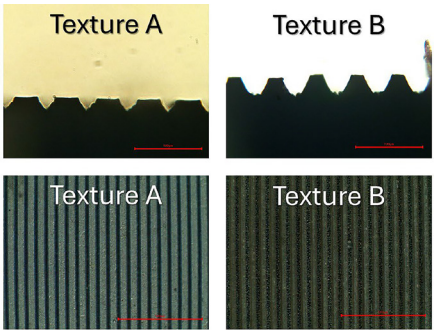

***Figure 2**. Optical microscopy images*
***Source:** developed by the authors of this study based on the findings of experimental research*

As illustrated in Figure 3, laser-induced textures were successfully transferred onto polymer substrates by three methods: reactive curing for silicone, solution casting for polycarbonate, and thermo-pressing for polyethylene. Each approach resulted in a clearly defined surface structure, enabling further comparison of replication fidelity and wetting behaviour. It can be concluded that all the replication methods enable a sufficiently accurate transfer of the texture. In particular, the periodicity was preserved, along with the regularity of the pattern and the groove width at the upper surface of the texture. When examining not only the top view of the textures but also their cross-sectional profiles, it became evident that different replication methods yield varying levels of fidelity. For instance, on polycarbonate negative, the apexes of the pyramidal structures were encrusted with artefactual formations originating from the focal points of the laser. These artefacts are relatively large – reaching up to 5 μm in height – and are distributed in a disordered manner across the surface. Similar artefactual formations can be observed for other samples. For polyethylene negative the pyramidal structures appear significantly narrower. This effect is primarily attributed to the use of an alternative template design featuring much narrower grooves. Notably, the artefactual formations have nearly disappeared, indicating that across the sequence of polycarbonate-polysiloxane-polyethylene there is a progressive reduction in the size of these extraneous features. This trend can likely be explained by the progressive increase in viscosity of the medium used for texture replication, moving from polycarbonate solution to liquid silicone resin and ultimately to molten polyethylene.

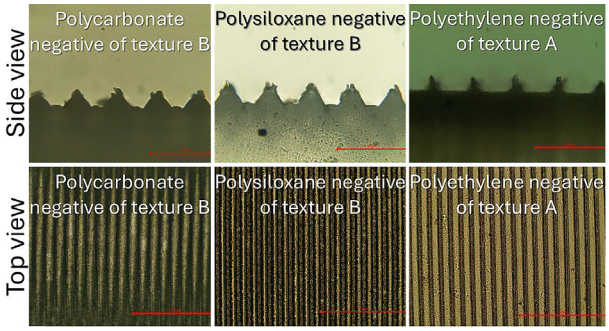

***Figure 3**. Textures obtained by templating from metal matrices*
***Source:** developed by the authors of this study based on the findings of experimental research*

Consequently, the lowest-viscosity system – namely, the polycarbonate solution in dichloromethane – exhibited the greatest ability to reproduce the fine surface features of the template with high fidelity. It should be emphasised that the presence of such artefactual formations on the textured surface is an undesirable factor. As demonstrated in earlier study by O. Myronyuk *et al*. (2024), these protrusions effectively reduce the maximum attainable water contact angle by destabilising the Cassie-Baxter state. They are expected to influence another critical parameter – the sliding angle strongly. Following the mechanism observed in the "rose petal" effect, these features enhance droplet pinning of the wetting liquid, thereby increasing the sliding angle. Thus, their presence is detrimental to the overall wetting performance of the surface. As can be seen from Figure 3, these artefacts are characteristic of nearly all surface replication methods employed. Consequently, relying solely on negative moulding from the template does not allow for the production of high-quality replicas with complete structural fidelity. Therefore, the authors of this study adopted a somewhat different approach. First, a negative template was prepared by a solution-based method using polycarbonate. This negative was then employed to generate positive structures from both a silicone polymer and polyethylene. In the former case, the replication was achieved through reactive moulding, while in the latter it was accomplished by thermo-pressing.

As shown in Figure 4, the positive replicas reproduced the original structure of the source templates with considerable accuracy compared to the metal substrates. Deep and highly accurate reproduction was achieved in both cases using polysiloxane polymer. This effect is particularly noticeable for texture A, where the dimensional characteristics are virtually identical to those of the original metal template, despite the fact that the structure was transferred through an intermediate polycarbonate negative.

The positive replica of texture B on polysiloxane differs slightly from the original template due to the presence of artificial concavity on the surface of the textured elements. Notably, this concavity is also present to a lesser extent in the original metal templates. The polyethylene replicas appeared less accurate, partly due to the visualisation conditions. In terms of dimensionality and geometry, it should be noted that the structural period and the crest-to-groove ratio remained unchanged for polyethylene and polysiloxane. The depth of the grooves was almost the same as that of the original structure. However, the angles and features were noticeably less distinct compared to the silicone body. This result was expected, as molten polyethylene has a significantly higher viscosity than liquid silicone during the moulding of these replicas.

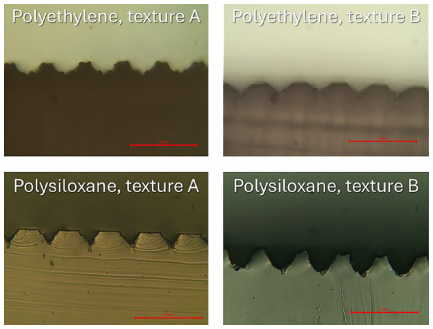

***Figure 4**. Side view of positive textures*
***Source:** developed by the authors of this study based on the findings of experimental research*

The parameters of structure transfer from the metallic master templates (AlSI304) with texture A and texture B onto polymer surfaces were presented in Table 2. Based on the data in the table, it is important to note that the negatives were obtained through direct contact of the polymers with the metallic templates, whereas the positives were produced by casting polyethylene and PDMS onto the surface of the polycarbonate negative. As a result, they also inherited the imprint of this intermediate template along with its associated modifications. For texture B, the polycarbonate negative exhibited certain alterations compared to the original template. First, there was a slight reduction in the height of the protrusions, although this decrease remained within the margin of experimental error. The textures exhibited a slight reduction in height, which can be attributed to the shrinkage of the polymer film following solvent evaporation. Moreover, it was observed that the width corresponding to the groove dimension in the positive replica remained unchanged, consistently measuring around 40 μm. The polysiloxane negative reproduced the template structure with nearly the same accuracy as the solution-cast polycarbonate. The only noticeable difference was that the grooves appear slightly deeper than those in the polycarbonate replica. However, this variation lied within the margin of error and can reasonably be attributed to statistical deviation.

The positive structures were of particular interest, as they represented the intended functional surfaces. Notably, the polysiloxane positive exhibited a slightly greater groove width, which arises from the corresponding broadening of the ridge elements in this replication process. Here, the difference was modest – 44 μm compared to 40 μm – yet it already lied beyond the range of statistical error. Thus, it can be concluded that during the moulding process certain effects, such as elongation upon demoulding or shrinkage, lead to a measurable narrowing of the ridge elements. This observation was further supported by the fact that the height of these ridges increased to 26.5 μm. However, the opposite trend was observed in another positive replica. Here, the ridge height decreased to approximately 20.5 μm, a change that also falls outside the bounds of statistical error. In addition, the ridge width showed a slight increase, although this variation remained within the margin of experimental uncertainty. Similar trends were also observed for texture A. Taller and more elongated ridges characterise the siloxane positive, whereas the polyethylene positive exhibits comparatively shorter ridge structures.

***Table 2**. Parameters of the texture grooves*

Texture	Material	Type	Groove width, μm	Groove depth, μm	Texture period, μm
A	AlSI304	positive	24.8 ± 2	19.5 ± 1	60 ± 2
B	AlSI304	positive	40 ± 1	24.5 ± 2	60 ± 1
A	Polyethylene	positive	36.5 ± 2	18.5 ± 1	58 ± 2
A	Polyethylene	negative	25.0 ± 1	23 ± 1.5	60 ± 1
B	Polyethylene	positive	37.5 ± 1.5	20.5 ± 1	58 ± 2.5
A	Polysiloxane	positive	30.0 ± 2	22.0 ± 1.5	59.5 ± 2
B	Polysiloxane	positive	44.5 ± 1.5	26.5 ± 2	58 ± 2.5
B	Polysiloxane	negative	39.0 ± 1.5	25.5 ± 2	57 ± 2.5
B	Polycarbonate	negative	39.5 ± 1.5	22.0 ± 1	57 ± 2.5

***Note:** negatives of polyethylene, silicone, and polycarbonate are presented only for texture "B" for the purpose of comparing transfer quality*
***Source:** developed by the authors of this study based on the findings of experimental research*

For the development of infused-liquid surfaces and superhydrophobic coatings, the key characteristics were defined by the wetting behaviour of the surface. This study examined how water wettability varies depending on the type

of structures that were fabricated. As shown in Table 3, the presence of surface texturing generally leads to an increase in the water contact angle of the materials in most cases. The flat surfaces exhibited a maximum water contact angle of approximately 103°, observed for polydimethylsiloxane. The textured surfaces exhibited enhanced contact angles regardless of whether they represented positive or negative replicas. The general trend showed that the perpendicular contact angles were only moderately higher than those of the flat surfaces, whereas in the case of parallel textures, the contact angles were significantly larger – by as much as 40° compared to the flat reference. This increase can primarily be attributed to the grooves themselves, which act as barriers to the spreading of the test liquid, in this case water, thereby generating a pronounced advancing angle that manifests as the measured static contact angle.

***Table 3**. Parameters of the texture grooves*

Texture	Material	Type	Orientation	Water contact angle, °
-	Polycarbonate	-	-	86.8 ± 2.2
-	Polyethylene	-	-	92.8 ± 0.6
-	Polysiloxane	-	-	102.7 ± 3.9
A	Polyethylene	positive	perpendicular =	102.4 ± 6.9
			parallel ||	130.6 ± 2.2
B			perpendicular =	137.4 ± 1.3
			parallel ||	138.8 ± 2.5
A	Polysiloxane	positive	perpendicular =	114.5 ± 1.7
			parallel ||	133.8 ± 2.1
B			perpendicular =	125.6 ± 0.9
			parallel ||	139.1 ± 1
A	Polycarbonate	negative	perpendicular =	91.0 ± 4.6
			parallel ||	127.4 ± 0.65
B			perpendicular =	60.7 ± 5.4
			parallel ||	111.2 ± 5.4

***Note:** "-" denotes samples without texture*
***Source:** developed by the authors of this study based on the findings of experimental research*

When comparing the efficiency of structures A and B, specifically their positive replicas, structure B proved to be more effective. In the parallel orientation, the polysiloxane sample – the most non-polar material – exhibited a maximum contact angle of approximately 140°, while polyethylene reached 139°. By contrast, structure A showed a lower maximum value, with the contact angle limited to about 134°. Based on data presented in Table 3, it can be concluded that the most effective configuration for enhancing water repellency is the positive replica based on structure B. Both polyethylene and polysiloxane proved to be highly promising materials for achieving elevated contact angles. In contrast, polycarbonate, owing to its higher polarity, is less effective in this regard. However, it serves excellently as an intermediate negative, as it reliably preserves the structural features of the original templates and enables the fabrication of highly reproducible positives from other polymers.

The results showed that the basic geometry of the textures was well preserved in all polymer replicas. However, artefacts with a diameter of up to 5 μm were observed at the top of the pyramidal elements in negative polycarbonate matrices, presumably due to the laser's action during focusing. Similarly, irregularities in replication were recorded in the study by V. Basile *et al*. (2022). Positive copies on polysiloxane were nearly identical to the original metal template; however, polyethylene replicas were less clear. The contours of the ridges were smoother, and the corners were less sharp due to the higher viscosity of molten polyethylene during thermoforming (Lysenkov & Strutskiy, 2022). Generally, as viscosity increases, the size and number of artefacts decrease; however, the replication accuracy of small details deteriorates. This was consistent with the observation of C. Sáez-Comet *et al*. (2022) that decreasing polymer viscosity (e.g., by increasing temperature) improves penetration into fine grooves and increases microtexture copying accuracy. Some parameters of the replicas differed systematically from the original. For instance, the width of the ridges in the polysiloxane positive for texture B increased from ~40 μm in the metal sample to ~44 μm, which can be explained by deformation during removal from the mould. The presence of artificial structures on surfaces can locally alter wetting angles, though it does not affect overall regularity. These differences suggest the effects of elastic recovery and shape change during cooling and material removal.

Surface texturing significantly increases the contact angle compared to flat samples. The Cassie-Baxter model explained this phenomenon: micro-roughness allows air to be retained in the depressions under the drop, increasing the macroscopic wetting angle (Ma *et al*., 2024). Additionally, pronounced anisotropy of wetting was observed: the angles measured parallel to the grooves were significantly higher than those measured perpendicular to them. Similar anisotropic wetting results were observed with micro-rough PDMS surfaces in Q. Legrand *et al*. (2022). As expected, structure B provided a higher contact angle than

structure A because more open-air area leads to a higher effective wetting angle according to the Cassie-Baxter model. Additionally, the nonpolar polysiloxane and polyethylene used to create the positives exhibited higher angles than the polar polycarbonate, consistent with these principles.

The presence of microartefacts was undesirable for water-repellent properties. As shown in the study by J. Bai *et al.* (2024), this leads to the "petal effect" a high static angle with high hysteresis. In other words, the surface becomes "stickier" for droplets. Contrary to the "lotus effect" irregularities impede the movement of the droplet. Y.B. Chatenet & S. Valette (2024) simulated the "lotus effect" and "petal effect" and showed that fluid penetration between irregularities in such micro-roughness leads to a decrease in the contact angle. Authors observations coincide with this: the presence of artefacts reduces the effectiveness of achieving the Cassie-Baxter state and increases excess hydrodynamic resistance. Therefore, smoothing or eliminating these structures is critical to manufacturing highly efficient superhydrophobic surfaces.

Thus, for the further advancement of research in this field, several strategies are recommended to enhance the water-repellent performance of textured surfaces. P. Gao *et al*. (2023) showed that the replication rate correlates with the viscosity of the polymer melt, which ensures a higher degree of polypropylene replication. D. Masato *et al.* (2022) proved that polymer deformation must be considered when separating the polymer from the metal template. Additionally, J. Krantz *et al.* (2022) proved in their study that the influence of temperature is significant. Thus, the use of lower-viscosity materials during moulding should be prioritised, which in thermoforming can be achieved either by increasing the processing temperature or by applying higher moulding pressure. The resulting textured surfaces may be further improved through post-processing hydrophobisation. I. Ramos *et al*. (2025) showed that the use of PDMS to impart hydrophobicity provides efficiency and durability. N. Rungruangkitkrai *et al.* (2024) showed that PDMS is a good alternative to fluorinated modifiers for creating LIPS materials. Although both polyethylene and PDMS are relatively nonpolar materials, they still possess a degree of surface polarity, and their hydrophobic properties can be significantly enhanced by additional surface modification.

Structure B provides higher contact angles than structure A, especially with less polar polymers like polysiloxane and polyethylene. Microtexture geometry is generally preserved during replication, though local microartefacts and deformations due to polymer viscosity and elastic recovery reduce accuracy. This aligns with the Cassie-Baxter model, which explains the increase in the contact angle due to air retention in microcavities and confirms the role of surface structure and material polarity in controlling wetting. Micro-irregularities beyond regular texture lead to a "petal" effect with increased hysteretic adhesion, reducing water-repellent properties. Optimising polymer melt viscosity during forming, controlling deformations during demoulding, and additional surface hydrophobisation are key strategies for improving superhydrophobic textured coatings.

Conclusions

The possibility of texture transfer onto polymer surfaces from textured metallic templates was demonstrated. The fidelity of replication is strongly influenced by the viscosity of the medium. Better replication quality was for polycarbonate solution. The accuracy of structure transfer increases to 5 μm with a decrease in viscosity, such as when switching from polymer melts and reactive mixtures to polymer solutions. In this study, a successful technological combination was demonstrated, whereby negatives were first fabricated by solution casting of polycarbonate, and these negatives were subsequently employed as templates for producing positive textured surfaces from polyethylene and polydimethylsiloxane.

During such transfers, the replicated structures exhibited distinct trends when compared to the original metallic substrates. First, the spacing between the texture ridges increased significantly – by up to 50% – and this effect was more pronounced for texture A (groove width 25 μm, groove depth 20 μm) than for texture B (groove width 40 μm, groove depth 25 μm). The increase was also more evident in the case of the highly viscous polyethylene than for polydimethylsiloxane, with changes of 50% and 25%, respectively. For texture B, the enlargement was much smaller, limited to about 10%. By contrast, the ridge height showed far less variation, with noticeable changes observed primarily in the polyethylene replicas.

It has been shown that surface texturing of polyethylene and PDMS leads to a substantial enhancement of their water-repellent properties. For instance, compared to flat polydimethylsiloxane, which exhibits a contact angle of 102°, the textured surfaces achieved values approaching 140°. This corresponded to an increase of close to 40° in the contact angle, clearly demonstrating the pronounced effect of texturing on wettability. The anisotropy of the texture also gives rise to anisotropy in the measured contact angles. For example, in the parallel orientation the contact angle reached approximately 140° for both polyethylene and polydimethylsiloxane, whereas in the perpendicular orientation the values decreased to approximately 125° and 137°, respectively. Further research should focus on determining the stability of infusion fluids in different textures and assessing their long-term stability under cyclic mechanical and chemical influences. These efforts will contribute to the practical applicability of slippery liquid-infused porous surface technology in operational conditions.

Acknowledgements

None.

Funding

This study was funded within the scope of the project # 2025.06/0031 "Polymeric liquid-infused films with de-icing

capability" (contract No. 217.0031 01.08.2025) by the National Research Foundation of Ukraine.

Conflict of Interest

None.

References

[1] Adera, S., Naworski, L., Davitt, A., Mandsberg, N.K., Shneidman, A.V., Alvarenga, J., & Aizenberg, J. (2021). Enhanced condensation heat transfer using porous silica inverse opal coatings on copper tubes. *Scientific Reports*, 11, article number 10675. doi: 10.1038/s41598-021-90015-x.

[2] Bai, J., Wang, X., Zhang, M., Yang, Z., & Zhang, J. (2024). Turning non-sticking surface into sticky surface: Correlation between surface topography and contact angle hysteresis. *Materials*, 17(9), article number 2006. doi: 10.3390/ma17092006.

[3] Basile, V., Modica, F., Surace, R., & Fassi, I. (2022). Micro-texturing of molds via Stereolithography for the fabrication of medical components. *Procedia CIRP*, 110, 93-98. doi: 10.1016/j.procir.2022.06.019.

[4] Bonse, J., Kirner, S.V., & Krüger, J. (2021). Laser-induced periodic surface structures (LIPSS). In K. Sugioka (Ed.), *Handbook of laser micro- and nano-engineering* (pp. 879-936). Cham: Springer. doi: 10.1007/978-3-030-63647-0_17.

[5] Cai, Q., Xu, J., Yu, Z., Dong, L., Li, J., Lian, Z., & Yu, H. (2023). Fabrication of slippery liquid-infused porous surfaces on magnesium alloys with durable anti-corrosion and anti-tribocorrosion properties. *Colloids and Surfaces A: Physicochemical and Engineering Aspects*, 670, article number 131549. doi: 10.1016/j.colsurfa.2023.131549.

[6] Chatenet, Y.B., & Valette, S. (2024). Elucidating the lotus and rose-petal effects on hierarchical surfaces: Study of the effect of topographical scales on the contact angle hysteresis. *Journal of Colloid and Interface Science*, 676, 355-367. doi: 10.1016/j.jcis.2024.07.114.

[7] Du, B., Zhou, X., Li, Q., Liu, J., Liu, Y., Zeng, X., Cheng, X., & Hu, H. (2023). Surface treat method to improve the adhesion between stainless steel and resin: A review. *ACS Omega*, 8(43), 39984-40004. doi: 10.1021/acsomega.3c05728.

[8] Etim, I.N., Zhang, R., Wang, C., Khan, S., Mathivanan, K., & Duan, J. (2025). New insights on slippery lubricant-infused porous surfaces technique in mitigating microbial corrosion. *Npj Materials Degradation*, 9, article number 34. doi: 10.1038/s41529-025-00581-y.

[9] Gao, P., MacKay, I., Gruber, A., Krantz, J., Piccolo, L., Lucchetta, G., Pelaccia, R., Orazi, L., & Masato, D. (2023). Wetting characteristics of laser-ablated hierarchical textures replicated by micro injection molding. *Micromachines*, 14(4), article number 863. doi: 10.3390/mi14040863.

[10] Krantz, J., Caiado, A., Piccolo, L., Gao, P., Sorgato, M., Lucchetta, G., & Masato, D. (2022). Dynamic wetting characteristics of submicron-structured injection molded parts. *Polymer Engineering and Science*, 62(7), 2093-2101. doi: 10.1002/pen.25983.

[11] Legrand, Q., Benayoun, S., & Valette, S. (2022). Quantification and modeling of anisotropic wetting of textured surfaces. *Applied Surface Science*, 611(B), article number 155606. doi: 10.1016/j.apsusc.2022.155606.

[12] Lysenkov, E., & Strutkyi, O. (2022). Electrical properties of polymer nanocomposites based on polyethylene oxide and silver nanoparticles in the area of low filler concentrations. *Bulletin of Cherkasy State Technological University*, 27(3), 94-101. doi: 10.24025/2306-4412.3.2022.262507.

[13] Ma, D., Liu, Z., Li, Y., & Luo, L. (2024). Experiment of droplet anisotropic wetting behavior on micro-grooved PDMS membranes. *Scientific Reports*, 14, article number 28011. doi: 10.1038/s41598-024-78681-z.

[14] Masato, D., Piccolo, L., Lucchetta, G., & Sorgato, M. (2022). Texturing technologies for plastics injection molding: A review. *Micromachines*, 13(8), article number 1211. doi: 10.3390/mi13081211.

[15] McHale, G., Ledesma-Aguilar, R., & Neto, C. (2023). Cassie's law reformulated: Composite surfaces from superspreading to superhydrophobic. *Langmuir*, 39(31), 11028-11035. doi: 10.1021/acs.langmuir.3c01313.

[16] Meng, Y., Xu, K., Li, S., Cao, H., Chen, C., Wei, Y., Wei, Y., & Tian, J. (2025). Slippery liquid-infused porous surfaces with long-term durable antifouling and anti-corrosion performance via bimodal structure design. *Surface and Coatings Technology*, 498, article number 131850. doi: 10.1016/j.surfcoat.2025.131850.

[17] Myronyuk, O., Baklan, D., & Rodin, A.M. (2023). UV resistance of super-hydrophobic stainless steel surfaces textured by femtosecond laser pulses. *Photonics*, 10(9), article number 1005. doi: 10.3390/photonics10091005.

[18] Myronyuk, O., Vanagas, E., Rodin, A.M., & Wesolowski, M. (2024). Estimation of the structure of hydrophobic surfaces using the Cassie-Baxter equation. *Materials*, 17(17), article number 4322. doi: 10.3390/ma17174322.

[19] Park, I.W., Ribe, J.M., Fernandino, M., & Dorao, C.A. (2023). The criterion of the Cassie-Baxter and Wenzel wetting modes and the effect of elastic substrates on it. *Advanced Materials Interfaces*, 10(12), article number 2202439. doi: 10.1002/admi.202202439.

[20] Peppou-Chapman, S., Hong, J.K., Waterhouse, A., & Neto, C. (2020). Life and death of liquid-infused surfaces: A review on the choice, analysis and fate of the infused liquid layer. *Chemical Society Reviews*, 49(11), 3688-3715. doi: 10.1039/d0cs00036a.

[21] Ramos, I., Gonçalves, M., Gonçalves, I.M., Carvalho, V., Fernandes, E., Lima, R., & Pinho, D. (2025). PDMS surface wettability modification and its applications: A systematic review. *Journal of Molecular Liquids*, 434, article number 127978. doi: 10.1016/j.molliq.2025.127978.

[22] Rungruangkitkrai, N., Phromphen, P., Chartvivatpornchai, N., Srisa, A., Laorenza, Y., Wongphan, P., & Harnkarnsujarit, N. (2024). Water repellent coating in textile, paper and bioplastic polymers: A comprehensive review. *Polymers*, 16(19), article number 2790. doi: 10.3390/polym16192790.

[23] Sáez-Comet, C., Fontdecaba, E., Cuadrado, N., & Puiggali, J. (2022). Injection molding and characterization of microtextures on polycarbonate using laser textured inserts. *Materials and Manufacturing Processes*, 38(5), 618-628. doi: 10.1080/10426914.2022.2075888.

[24] Tripathi, D., Ray, P., Singh, A.V., Kishore, V., & Singh, S.L. (2023). Durability of slippery liquid-infused surfaces: Challenges and advances. *Coatings*, 13(6), article number 1095. doi: 10.3390/coatings13061095.

[25] Xie, H., & Huang, H. (2020). Gradient wetting transition from the Wenzel to robust Cassie-Baxter states along nanopillared cicada wing and underlying mechanism. *Journal of Bionic Engineering*, 17, 1009-1018. doi: 10.1007/s42235-020-0080-x.

Формування мікротекстур полімерних поверхонь методом переносу з металевих шаблонів

Олексій Миронюк
Доктор технічних наук, доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0003-0499-9491
Денис Баклан
Доктор філософії
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-6608-0117
Анна Білоусова
Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-2818-8450
Володимир Страшенко
Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0009-0009-3601-1821

Анотація. Масштабування технологій створення рельєфних поверхонь з контрольованими властивостями змочування є актуальним завданням для розвитку функціональних полімерних матеріалів. Існує необхідність вивчення закономірностей перенесення мікро- та нанотекстур з металевих шаблонів на полімерні підкладки. Метою роботи було визначення впливу методу реплікації та властивостей полімеру на точність відтворення рельєфу та формування водовідштовхувальних характеристик поверхні. Для цього було використано три методи реплікації: отримання полікарбонатної плівки з розчину, реакційне формування з використанням еластомеру полідиметилсилоксану та термоформування поліетиленових плівок. Отримані негативні копії використовували як проміжні форми (полікарбонат) для створення позитивних реплік з поліетилену та полісилоксану. Гідрофобність матеріалів оцінювали шляхом вимірювання кутів контакту в напрямках, паралельних і перпендикулярних до орієнтації текстури. Результати показали, що всі методи забезпечують відтворення періодичних структур. Однак рівень точності залежить від в'язкості середовища та температурних умов, причому найнижчий рівень точності спостерігається для полікарбонату, а найвищий – для поліетилену. Полікарбонатні негативи характеризувалися високою деталізацією мікродефектів (до 5 мкм), тоді як поліетиленові плівки демонстрували згладжування рельєфу. Силіконові позитиви найбільш повно зберігають геометрію оригінальних текстур з дефектами. Дослідження гідрофобності поверхні показало значне збільшення кутів контакту на структурованих поверхнях порівняно з гладкими, особливо при паралельній орієнтації. Максимальні кути контакту досягали 140 °C для полісилоксану і 139 °C для поліетиленових реплік структури з регулярними канавками. Практична цінність роботи полягала у визначенні оптимальних матеріалів і методів для створення полімерних поверхонь з підвищеною водовідштовхувальною здатністю. Полікарбонат підходить для використання як проміжний матеріал для точного копіювання текстури, тоді як силікон і поліетилен мають потенціал для використання як функціональні поверхні в захисних покриттях і пористих поверхнях, просочених рідиною

Ключові слова: кут змочування; полікарбонат; силікон; поліетилен; гідрофобність

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 17.04.2025
Revised: 15.08.2025
Accepted: 17.09.2025

UDC 004.9

DOI: 10.30857/2786-5371.2025.4.5

Conceptual model of a web-based traffic flow management system in an urban environment based on microservice architecture

Andrii Roskladka*

Doctor of Economic Sciences, Professor
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0000-0002-1297-377X

Yevhenii Postrelko

Postgraduate Student
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0000-0001-9730-450X

Abstract. The relevance of the research arises from the growing load on urban transport infrastructure, the need for digital transformation of mobility management, and the implementation of intelligent data analytics technologies operating in real time. Such a system enables prompt responses to changes in traffic conditions, improves the efficiency of the route network, and enhances the overall quality of urban transportation services. The purpose of the study was to design the architecture of a web system that ensures the integration of data from city application programming interfaces, their automated processing, analytical interpretation, visualisation of results, and centralised configuration management. The methodological basis of the research included approaches of systems analysis, data flow modelling, the construction of entity-relationship diagrams, and the use of architectural design patterns to represent the structural and functional interaction of components. The article presented the development of a conceptual model of a web-based system for managing traffic flows in an urban environment, designed according to the principles of microservice architecture. The research outcome was the creation of a structural model of the system comprising five interrelated microservices: integration with city application programming interfaces (Node.js), data processing and aggregation (Python, Redis Streams), an analytical module with machine learning algorithms (Scikit-learn), a visualisation module (React, Mapbox, Chart.js), and a service for access control and configuration management. The paper provided a detailed description of their interaction logic, scaling mechanisms, and reliability assurance. The practical value of the study lied in the development of a universal architectural framework for implementing systems of analytics and monitoring of urban transport, which may serve as a prototype for intelligent mobility management platforms within the Smart City concept

Keywords: distributed information services; digital modelling of urban mobility; real-time data flow analysis; web analytics of transport systems; spatio-temporal data visualisation; Smart City

Introduction

Rapid urbanisation and the saturation of transport infrastructure require cities to adopt flexible digital solutions capable of handling large-scale data streams in near real time. Traditional monolithic approaches do not provide the necessary scalability, fault tolerance, or speed of deployment. By contrast, a microservice architecture, combined with web technologies and contemporary analytics, enables the development of manageable, transparent, and reproducible systems for traffic flow management at the urban scale. In this context, articulating a concept that links data acquisition, processing, analytics, and presentation within a coherent architectural frame becomes essential for reproducibility and future scaling.

Ukrainian and international scholars are actively advancing research on web architecture, microservices, traffic flow management, visual analytics, and the Smart City

Suggested Citation:
Roskladka, A., & Postrelko, Ye. (2025). Conceptual model of a web-based traffic flow management system in an urban environment based on microservice architecture. *Technologies and Engineering,* 26(4), 54-67. doi: 10.30857/2786-5371.2025.4.5.

*Corresponding author

paradigm. Ukrainian researchers M. Kotenko *et al*. (2024) have systematised security practices for microservice architecture – including service mesh, mutual Transport Layer Security, Zero Trust, and Development, Security, and Operations – demonstrating their practical value for building secure, distributed web systems. Their work emphasised layered defences (isolation, Application Programming Interface (API) gateways, policy-based access) and showed how service mesh patterns reduce the attack surface and centralise traffic governance in distributed environments, which is crucial for city-scale web platforms handling personal mobility data. D. Volkov & V. Liubchenko (2024) provided a review of threats and protection strategies for microservices and identified gaps in their application; their study underscored the importance of comprehensive risk-management approaches within microservice architecture and established a methodological foundation for the secure integration of urban transport services. In particular, they highlighted the absence of universal threat models for microservices and advocate STRIDE-oriented (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) analysed coupled with container hardening and secure inter-service communication, aligning well with transport systems that must assure integrity and availability during peak loads or incidents. Y. Matseliukh & V. Lytvyn (2024) proposed a model for analysing passenger flows in low-carbon transport within a Smart City, and outlined a sequence of data sources and open datasets that are particularly useful for urban transport visualisations. Their correlation-regression analysis connected passenger throughput with CO_2 emissions, motivating analytics modules that not only forecast flows but also assess ecological impact; this directly informs key performance indicators sets for dashboards in a traffic management web system (e.g., trip time, occupancy, emission proxies). Y. Ohonovskyi *et al*. (2023) presented a prototype of an information system for monitoring and content analysis of citizens' appeals in a Smart City context, with an emphasis on web-oriented integration of municipal services. The proposed ideas proved suitable for composing a web platform for flow management with modular integration of urban data. This citizen-feedback channel complements sensor data: incident reports, complaints, and requests create additional signals for congestion detection and service prioritisation, which a microservice platform can ingest via dedicated ingestion and natural language processing services. A. Danyliuk & O. Muliarevych (2024) examined approaches to traffic control, including Cyber-Physical Systems/Internet of Things (CPS/IoT) solutions and elements of artificial intelligence; these approaches helped to establish the algorithmic context for the analytical microservice of the web system. Their surveys of adaptive signal control and parameter sets (speed, density, volume) provided a catalogue of measurable features that can be operationalised in forecasting pipelines, while the CPS perspective clarifies integration patterns with roadside devices through secure APIs. Building on systems analysis, O. Barabash *et al*. (2021) decomposed the urban transport system, developed a road-safety profile, and outlined criteria for flow efficiency, while separately highlighting the role of, and risks posed by, telecommunication threats. Their "traffic safety profile" concept suggested a morphology of factors (network design, intersection typology, pedestrian streams) that can be encoded as domain ontologies and used for rule-based diagnostics in tandem with predictive models. Y. Fornalchyk & V. Hilevych (2023) demonstrated that increasing motorisation correlates with higher accident rates, noise, and emissions, and substantiated a transition towards an artificial-intelligence-enabled transport network with centralised monitoring as a viable direction for mitigation. This evidence strengthened the case for city-wide coordination layers in the architecture (control plane plus monitoring plane) to mitigate externalities of motorisation through proactive forecasting and targeted control policies.

Y. Yu *et al*. (2025) systematised visual analytics techniques for heterogeneous mobility data, highlighting, among the principal visual objects, origin-destination maps, a range of progressive analytics methods, and inclusive interface designs. Their InclusiViz system combined deep models (Deep Gravity-style) with explainable analytics and what-if tooling, indicating how a traffic platform may evolve from descriptive dashboards to prescriptive, simulation-backed decision support with multi-level views (city-wide to neighbourhood). A. Wibowo *et al*. (2024) proposed the MxT model, which integrates streams from the X social network to detect obstructions and enable rapid route adjustments; their results reported over 91.6% detection accuracy and approximately a 15% reduction in travel time. This illustrated a viable "social sensing" microservice that enriches sensor feeds during disruptions (floods, protests), with grounding via ground-truth validation – an approach transferrable to European cities with similar incident typologies.

Building on the outlined problematisation, the study aimed to propose a coherent conceptual model of a web-based traffic flow management system for the urban environment, grounded in microservice architecture, which aligns data acquisition and integration with their analytical interpretation, visualisation, and the administrative management of configurations.

Materials and Methods

This article presented an original conceptual model developed within a design-science approach. The research methodology comprised several consecutive stages. Based on a review of publications and practical cases in urban mobility management, the functional zones of the system were identified: data acquisition and integration, data processing and aggregation, analytics, visualisation, and access and configuration. These zones were then used as criteria for the architectural design. The system was decomposed into five microservices that correspond to these zones, and their structure and interactions are described in the sections devoted to individual microservices. For each

functional zone, a set of entity-relationship (ER), data-flow diagrams (DFD) and context-container-component-code (C4) diagrams was prepared to capture the domain structure, information flows and boundaries of microservice responsibility. The final stage was a qualitative comparison of candidate analytical tool stacks (Python, R, Excel/Power BI) using criteria such as performance, scalability and suitability for integration into a microservice architecture.

The conceptual model was developed as a sequential architectural design process with the key artefacts explicitly documented. The architectural solution followed a "context → containers → components" approach. Microservices were distinguished for integration with municipal APIs (data ingestion and dissemination), data processing and aggregation (validation, normalisation, and consolidation of indicators), analytics (calculation of indicators and support for forecasting algorithms), visualisation (maps and charts for presenting results), and access and configuration management (centralised settings and access rights). For each microservice, public interfaces and message exchanges were specified to ensure independent evolution of components and their scalability.

In constructing the conceptual model, the focus was on defining data schemas, interfaces and information flows at the architectural level. No concrete test datasets or quantitative experiments with real or synthetic records were designed within this study. In the conceptual model, a separate functional zone is formed by the results visualisation layer, which is responsible for presenting aggregated and analytical data in a clear form for different groups of users. To provide a coherent representation of the structure and information flows, a domain ER diagram was created (routes, stops, vehicles, traffic events, indicators/forecasts, users/roles, configurations), as well as DFD for levels 0-2 (the main channels of data ingestion, processing, and delivery) and a C4 diagram that shows microservice responsibility boundaries and their interactions. Together with interface specifications and data format descriptions, these diagrams enable other researchers to reproduce the proposed model under comparable conditions. The reproducibility of the solution was supported by documenting interface schemas, canonical definitions of indicators, and typical configurations, so that equivalent deployments can be implemented in different urban contexts without changing the underlying architectural principles.

Results and Discussion

Municipal API integration microservice. The system comprises distinct microservices, each responsible for a specific set of functions: integration with municipal APIs, data processing and aggregation, analytical computation, results visualisation, and configuration management. The municipal API integration microservice is intended to ingest, process, and preliminarily validate data on intra-urban traffic flows. Its primary task is envisaged to be the establishment of stable communication with external services that are expected to provide up-to-date information on public transport movements, routes, timetables, and potential delays. In the conceptual model, the microservice is designed to perform regular or event-driven requests to designated APIs, as discussed by A. Bokolo (2025), who emphasised the role of RESTful integration patterns for Smart City data exchange, ensuring the processing of received data and their transformation into an internal format suitable for further analytical interpretation.

Introducing a dedicated microservice for API integration is meant to enable high flexibility when data sources or response formats change, while minimising the impact on other components of the web system. Moreover, isolating data acquisition into an independent service is intended to enhance the solution's scalability and to simplify its maintenance; G. Şahin *et al*. (2024) outlined similar benefits of decoupled ingestion layers for maintainability and scale in municipal web systems.

In implementing the project, it is assumed that the developers will have access to open APIs of municipal transport services that provide the necessary information in a specified format. In particular, it is envisaged that the APIs support standard HTTP (HyperText Transfer Protocol) requests (GET method) and return responses in JSON (JavaScript Object Notation) containing the following key attributes: a unique vehicle identifier; geographic coordinates (latitude, longitude); current speed; route identifier; scheduled arrival time at the next stop; actual timestamp of the latest update. The Municipal API Integration microservice is positioned to play a critical role in ensuring reliable acquisition of traffic-flow data for subsequent analysis. Its principal functional components are proposed to include:

1) Initiation of requests to open municipal APIs. The microservice is expected to periodically issue HTTP requests (predominantly via the GET method) to designated municipal API endpoints to retrieve vehicle locations, routes, and timetables. A standardised REST architecture is intended to underpin this integration, consistent with contemporary Smart City practice; A. Bokolo (2025) underscored that consistent REST conventions improve interoperability and reduce coupling across civic data services.

2) Validation and verification of received data. Responses are to be checked against the expected structure, including the presence of mandatory fields (vehicle identifier, coordinates, speed, update time). In the event of malformed or incomplete records, the microservice is expected to filter them out to maintain a high level of information quality; I.M. Leghemo *et al.* (2025) drew attention to systematic quality gates for API-delivered mobility streams.

3) Transformation into an internal unified format. To ensure interoperability, data obtained from heterogeneous APIs are intended to be normalised to a predefined schema. This is meant to prevent errors during subsequent processing and visualisation.

4) Error handling and resilience. When an external API is unavailable or returns an invalid response, the microservice applies retry mechanisms with exponential backoff and emits error notifications for downstream auditing.

5) Real-time or scheduled data refresh. The microservice is designed to support both event-driven processing (e.g., upon receipt of an update signal) and periodic data collection at a configured interval, which is expected to enable optimisation of system load.

Thus, the integration microservice is expected to ensure reliable ingestion, validation, and preparation of transport data for subsequent analytical and visualisation processes within the web-based traffic flow analysis system. Implementing the municipal API integration microservice is assumed to require technologies capable of sustaining high throughput under large volumes of concurrent requests, offering flexibility in API handling, and ensuring robust data processing. Following a comparison of several technology stacks, the development would adopt Node.js with the Axios library for issuing HTTP requests. This choice is justified by Node.js's efficiency in handling asynchronous calls through its non-blocking I/O model, as highlighted by B.S. Beeraka (2025), who associated event-driven runtimes with high-frequency HTTP workloads in urban analytics, which is considered critical for tasks characterised by high-frequency data exchange.

The chosen Node.js technology is expected to enable the microservice requirements to be met effectively in terms of request processing speed, ease of API integration, and scalability under increasing load. A conceptual container diagram (Fig. 1) is intended to illustrate the architecture of the municipal API integration microservice implemented in the proposed stack. In this diagram, the microservice establishes connections to external APIs, handles requests, transforms data into the internal format, validates the retrieved information, and persists it for subsequent processing within the traffic flow analysis system.

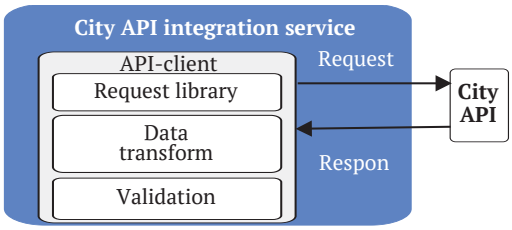

***Figure 1**. Container diagram of the Municipal API Integration microservice*
***Source:** designed by the authors*

In summary, the municipal API integration microservice is intended to provide a stable, configurable entry point for mobility data, decoupling external API variability from the system's internal contracts. Its design is expected to prioritise ingest throughput, schema normalisation, and explicit error-handling paths so that downstream services receive consistent, high-quality records. Operationally, the service is envisaged to support both scheduled and event-driven refresh modes, enabling cities to balance latency against load. By isolating acquisition concerns and exposing a narrow, well-typed interface, the microservice is intended to simplify maintenance, support independent scaling, and reduce the blast radius of upstream changes. Collectively, these properties are expected to improve reliability and to create a robust foundation for subsequent aggregation, analytics, and visualisation.

Data processing and aggregation microservice. The data processing and aggregation microservice is a key component that is intended to perform the initial processing of data received from the Municipal API Integration microservice. E. Puzio *et al.* (2025) described analogous staging of pre-analytics pipelines for transport feeds, which motivates the separation of ingestion and cleaning as a distinct service layer. Its primary purpose is to render the data into a structured form suitable for subsequent analysis, storage, and visualisation. This is envisaged to be achieved by filtering out malformed or incomplete records, normalising value formats (e.g., time and coordinates), consolidating data by routes, vehicles, or time intervals, and computing basic aggregates (such as average speed and mean delay). Thus, the microservice is positioned to serve as a buffer between raw, unprocessed data and the analytics modules, providing a reliable, high-quality foundation for all subsequent computations within the system.

Within this microservice, it is assumed that the input arrives as structured JSON objects from the preceding integration microservice and contains the following attributes: a unique vehicle identifier; a route identifier; the data capture time in Coordinated Universal Time (UTC); location coordinates; current speed; delay, in minutes, relative to the timetable. Based on the input data, aggregation is intended to be performed by routes; by time intervals; by geographical zones. As a result, analytical slices are expected to be produced that include, inter alia: average speed on a route over the selected period; frequency of stops or delays; number of active vehicles at a given moment. After aggregation, the data are to be stored in a standardised internal format (e.g., as JSON objects or database tables), facilitating seamless integration with subsequent system modules (analytics and visualisation). The Power BI Community (2021) outlined practical constraints of spreadsheet-centric pipelines for streaming data, and N.O. Quesado Filho *et al.* (2025) contrasted dashboard tooling with code-first stacks, which together support the decision to separate Extract-Transform-Load (ETL)-like routines from end-user visualisation layers. A comparison of these options according to the criteria of performance, flexibility, scalability and support for machine learning tools is provided in Table 1.

***Table 1**. Comparison of analytical tools for implementing a web system*

Criterion	Python	R	Excel / Power BI
Computing performance	High (vectorisation, NumPy)	Average, good for statistics	Low, not suitable for large volumes
Libraries for machine learning/AI	Scikit-learn, XGBoost, Prophet	Caret, GTFSwizard, Forecast	Minimum (statistics only)

Table 1. Continued

Criterion	Python	R	Excel / Power BI
Working with spatial data	GeoPandas, Folium	SF, Leaflet, GTFSwizard	Only through external plugins
Integration into a microservice system	High (FastAPI, Flask, Celery)	Limited, harder to scale	Not intended for server systems
Learning curve	Moderate	Moderate	Low
Open code	Yes	Yes	Partially (closed formulas)

Source: *compiled by the authors*

Although R is noted to have a few quality libraries for analysing GTFS transport data (e.g., GTFSwizard), its weaker representation in microservices and web integration ecosystems is assumed to limit its use for real-world deployment of transport analytics. Using Excel/Power BI is considered justified in cases of visual data analysis for non-specialists, however, this approach does not scale, offers limited automation, and does not support the flexible application of machine learning algorithms. Python is considered to have an advantage in all key aspects: computational speed, support for machine learning libraries; integration with infrastructure components (FastAPI, Celery); flexibility of spatial analysis (GeoPandas, Shapely).

For implementing the data processing and aggregation microservice, the Python language was selected conceptually, as its libraries are intended to provide high efficiency when working with data arrays – specifically, pandas for tabular processing, NumPy for numerical operations, and datetime for time-interval manipulation. Python is chosen for its optimal balance between syntactic simplicity, a broad toolkit for data analysis, and straightforward integration with streaming solutions (e.g., Redis Streams or Apache Kafka). Compared with other languages (such as Java or Scala), Python is considered more suitable for prototyping and for flexible handling of semi-structured data, which are typical of transport analytics. K.Ntouros *et al.* (2025) emphasised the practical advantages of Python-centric data engineering for municipal platforms, a consideration reflected in the prioritisation of a lightweight but extensible stack. As the data-streaming system, Redis Streams is considered due to its lightweight nature, rapid deployment, and minimal configuration requirements. This is particularly advantageous in urban settings, where the system is expected to operate with reduced latencies and respond swiftly to incoming records. F. Yang (2025) highlighted the utility of stream abstractions that combine event buffering with time-windowed aggregation, a capability mirrored by Redis Streams for transport-data grouping.

The data processing and aggregation microservice is positioned to play a critical role in transforming raw information on traffic flows into aggregated, clean, and structured data that can be used directly for subsequent analysis and visualisation. Its architecture is intended to enable the efficient detection of anomalous values, the grouping of data by routes, vehicles, or time intervals, and the construction of core metrics – average speed, delays, and the number of active vehicles. Taken together, these design choices are expected to provide an optimal balance between performance, implementation simplicity, and adaptability to data volumes, thereby delivering a scalable foundation for further integration with the system's analytics and visualisation modules (Horokhovskyi & Oshovska 2015). The diagram (Fig. 2) was intended to depict the principal stages of transport data processing within the microservice implemented in Python, using Redis Streams as the streaming mechanism. Input data are assumed to enter Redis Streams, where they are buffered and forwarded to the processor. The workflow is expected to perform filtering, normalisation, and aggregation, followed by grouping by routes, time intervals, or geozones. The aggregated results are to be stored in the internal repository (Redis JSON) and prepared for subsequent use by other system modules.

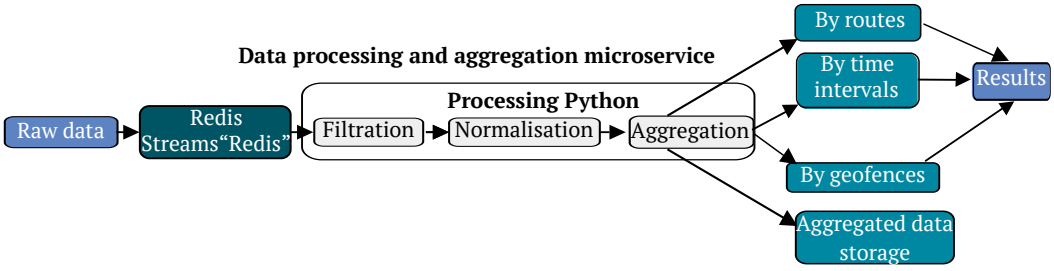

Figure 2*. Microservice architecture for data processing and aggregation*

Source: *designed by the authors*

In summary, the data processing and aggregation microservice is intended to act as the system's stabilising layer, converting heterogeneous, event-level inputs into consistent, analysis-ready datasets. Its workflow prioritises deterministic cleaning rules, schema normalisation, and configurable aggregation windows so that downstream modules receive comparable indicators across routes, times, and zones. By separating operational

(near-real-time) and periodic (batch) modes, the service is expected to balance latency with completeness and to prevent contention under peak loads. The explicit generation of core metrics – such as average speed, delay distributions, and active-vehicle counts – provides a minimal yet sufficient feature set for forecasting and visualisation. Collectively, these properties are intended to reduce error propagation, simplify debugging, and create a scalable foundation for the analytical and presentation layers.

Analytics microservice for urban transport analytics and forecasting. The analytics microservice is a key component of the web-based traffic flow analysis system, as it is intended to enable the transition from aggregated data to practically meaningful insights. This component is designed to process cleaned and structured data to identify patterns, forecast problematic segments, and formulate hypotheses for improving the city's route network. In contrast to the Data Processing and Aggregation microservice, the analytics module is oriented not only toward handling current values but also toward generating conclusions that may have strategic significance for urban mobility planning. The analytics microservice is assumed to perform intelligent processing of aggregated transport data to detect anomalies, derive performance indicators, and generate forecasts of load across the city's route network. It operates conceptually on data prepared by the preceding microservices, which are expected to supply cleaned, structured time-series information on vehicle movements.

The microservice is designed to perform in-depth analytics of transport data, specifically: detecting congestion and zones of heightened traffic intensity; analysing deviations from timetables and delays in public transport; computing route efficiency metrics (e.g., load factor, average travel time); producing baseline forecasts of delays or route load for specified periods; generating a set of recommendations (hypotheses) for the optimisation of the transport network. Thus, the analytics microservice is intended to provide the intelligent data processing required for well-founded managerial decisions in urban transport. Within the analytics microservice, it is assumed that the inputs are the aggregated and normalised datasets produced by the preceding Processing and Aggregation microservice. These data are expected to be error-cleaned, structured by key parameters, and ready for analytical interpretation. A basic input structure may be represented as a table or as JSON objects with the following records: route identifier; time interval; average speed on the route for the corresponding interval; average deviation from the timetable; number of vehicles on the route; route load factor; territorial zone or city sector. All records are to be generated with a uniform temporal step, which is intended to enable the construction of time series, the application of cluster or correlation analysis, and the assessment of indicator dynamics over time.

One of the module's principal functions is envisaged to be the detection zones of heightened traffic load – that is, segments characterised by persistently low average speeds combined with a high number of vehicles. To this end, filters are intended to be applied to identify critical speed thresholds, or cluster analysis is to be employed to delineate typical traffic situations across the city. A.O. Oyenuga *et al.* (2025) described comparable urban-mobility analyses that translate such clusterings into resource-allocation signals for city operations, which informs the choice to keep the feature space compatible with route-level interventions. Another function of the microservice is proposed to be the analysis of deviations from public transport timetables. For this purpose, the microservice is expected to compare the actual and scheduled times at stops. The results are intended to enable an assessment of delay levels by day of the week and by time interval, to identify peak periods of instability, and to localise zones where timetable violations are systematic. Where additional data become available, such as weather or event calendars, these factors are intended to be incorporated as covariates in regression-style models, following practice outlined by E. Erişkin (2024) for transport-policy evaluation. A dedicated functional block is assumed to be responsible for computing route efficiency, including the calculation of average travel time, a regularity coefficient (the ratio of actual to scheduled arrivals), speed variance, and route load levels across different times of day. These indicators are intended to allow for a quantitative assessment not only of the stability but also of the predictability of public transport operations.

In subsequent iterations, the microservice is intended to incorporate a forecasting module for delays or congestion. This can be achieved by building time-series models (e.g., Seasonal AutoRegressive Integrated Moving Average – SARIMA) or by applying machine-learning methods (such as linear regression or eXtreme Gradient Boosting (XGBoost)) to predict metric values for the subsequent hours or days. N. Schetakis *et al*. (2025) discussed short-term transport forecasting pipelines where classical time-series baselines remain competitive under constrained data, which motivates the decision to stage SARIMA alongside tree-based learners. S.A. Inamdar & S.S. Kulkarni (2025) explored quantum-inspired variants for near-term improvements; in the case of this article, such methods are regarded as future options once a stable benchmark is established. The final stage of the analytics microservice is envisaged to involve generating hypotheses for the optimisation of the transport network. Drawing on analyses of congestion, delays, and related metrics, the microservice is expected to propose adjustments to the route network – for example, relocating or adding stops, modifying headways, or introducing additional services during peak hours. All hypotheses are intended to be logged and prioritised by criticality, with forwarding to an administrative console for expert review. Thus, the analytics microservice enables the transition from aggregated data to concrete managerial conclusions that may be applied both to the tactical regulation of traffic and to the strategic planning of urban mobility.

The diagram (Fig. 3) was intended to depict the structure for processing aggregated transport data within the analytics microservice. Input data in JSON or comma-separated values (CSV) format are assumed to be received from the preceding Processing and Aggregation module. In the first stage, key metrics are expected to be computed (average speed, delays, traffic intensity), after which congestion and unstable routes are intended to be identified. Where required, the forecasting module is planned to be activated, employing machine-learning or time-series algorithms. The final stage is intended to generate hypotheses for improving the route network. The results are to be passed, as structured JSON objects, to the subsequent components of the system.

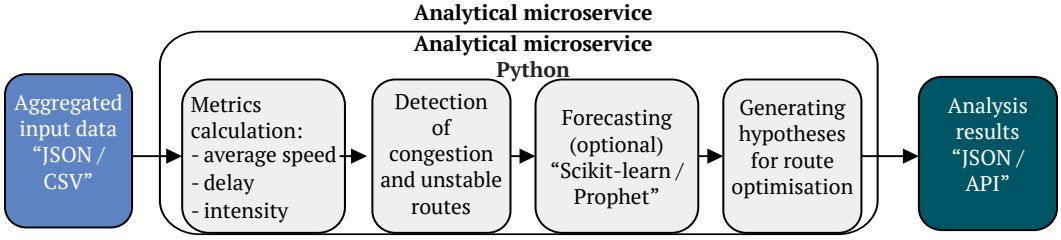

***Figure 3**. Analytical microservice architecture*

***Source:** designed by the authors*

For the implementation of the analytics microservice, a technology stack is proposed that is oriented towards efficient handling of tabular and time-series data, mathematical modelling, and machine learning. Python is positioned to serve as the primary implementation language, being widely adopted in urban and transport analytics and allowing a rapid transition from prototypes to reproducible pipelines. Y. Yu *et al.* (2025) illustrated how Python ecosystems – pandas for feature engineering and scikit-learn for modelling – can underpin multi-level mobility visualisation with explainable components, which aligns with design of this study for a modular analytics layer. The suite of specialised Python libraries is intended to enable both basic statistical processing and more advanced models for analysing temporal trends and forecasting. In particular, the InclusiViz line of work by the same authors demonstrated that code-first stacks facilitate consistent metric definitions across maps and charts, an approach authors of this study planed to mirror to maintain indicator reproducibility.

In the domain of policy-facing forecasting and optimisation, E. Erişkin (2024) showed that Python pipelines can blend behavioural covariates (e.g., weather, event calendars) with machine-learning baselines for transport strategy appraisal; the feature space is therefore planned to remain extensible so that such covariates can be incorporated without altering service boundaries. For real-time or near-real-time processing, the analytics microservice is intended to interface with streaming sources (e.g., Redis Streams), or to operate on periodically updated JSON/CSV files or tables supplied by the preceding microservice. F. Yang (2025) emphasised the advantage of stream abstractions that combine event buffering with windowed aggregation; this insight motivates authors' choice to expose time-window parameters at the configuration level so that cities can tune latency versus completeness. The selected stack is expected to enable the processing of large volumes of transport data, the scaling of computations as load increases, and the seamless integration of the results with the system's visualisation and administration microservices.

To support spatial analysis, the stack is intended to include GeoPandas for topology-aware joins and Shapely for geometric operations, enabling, for instance, corridor-level congestion detection and zone-based aggregation without bespoke Geographic Information System (GIS) servers. K. Ntouros *et al.* (2025) argued for lightweight, Python-centric data engineering in municipal platforms, noting that such stacks reduce operational overhead while preserving extensibility; this perspective underlies authors' preference for a lean but composable toolchain. Where higher-throughput ingestion becomes necessary, the microservice boundary is planned to admit Kafka-style brokers, yet the baseline remains deliberately minimal to keep deployment attainable for smaller cities.

Model selection for short-term forecasting is intended to balance classical time-series methods (e.g., SARIMA) and non-linear learners (e.g., gradient-boosted trees such as XGBoost) so that the system can operate under both scarce-data and richer-feature scenarios. N. Schetakis *et al.* (2025) reported that well-tuned classical baselines remain competitive when observation windows are short or sensors are uneven, which informs authors' decision to stage SARIMA alongside machine-learning alternatives rather than replacing them outright. Exploratory tracks, including quantum-inspired variants discussed by S.A. Inamdar & S.S. Kulkarni (2025), were considered future options once deterministic benchmarks are established and validated against municipal ground truth. Taken together, the proposed Python-first stack is intended to provide a pragmatic compromise: rapid prototyping for research iterations, explicit contracts for service integration, and a clear path to scaling analytics as cities expand data coverage and latency expectations.

In summary, the analytics microservice is intended to convert cleaned, aggregated streams into decision-ready insights by combining descriptive indicators, anomaly

detection, and short-term forecasting within one configurable pipeline. Its design is expected to preserve reproducibility through uniform time steps, stable metric definitions, and explicit feature schemas, while accommodating both near-real-time updates and periodic batch analyses. By emitting compact outputs – congestion flags, timetable-stability scores, route-efficiency metrics, and ranked optimisation hypotheses – the service is positioned to support both operational interventions and longer-horizon planning. Clear JSON contracts and stateless execution paths are envisaged to ease integration with visualisation and administrative layers, enabling independent scaling as data coverage grows. Collectively, these properties are intended to improve interpretability, shorten feedback loops for transport managers, and provide a robust analytical core for the overall system.

Visualisation microservice for interactive urban mobility dashboards. The visualisation microservice is intended to serve as the terminal presentation layer for all processed information in the system, transforming analytical and aggregated data into clear, interactive visual components. Its principal aim is to provide convenient, intuitive access to complex transport information for a broad range of users – from municipal analysts to ordinary citizens and transport operators. D.M. Kozachenko *et al.* (2025) argued that user-centred map interfaces improve decision latency for operational staff, which underpins the choice to emphasise rapid situational awareness over purely exploratory views. The scope of responsibility is proposed to include building interactive maps with public transport routes, congestion, and stops; displaying charts of headways, average speed, delays, and passenger volumes; generating heat maps of transport load across different times of day; presenting graphical analytics outputs in the form of diagrams, histograms, and time series.

Thanks to this microservice, users are expected to be able to review the current state of the transport situation, analyse its dynamics, compare data across periods, detect anomalies, and support well-founded decisions. Within the visualisation microservice, inputs are assumed to arrive from the analytics microservice and from the store of aggregated data. These inputs adhere to a standardised format suitable for subsequent rendering in the web interface. The data are intended to be provided as Geospatial JSON (GeoJSON) objects for mapping routes, stops, and vehicles; JSON tables or arrays for time charts, delays, and traffic intensity; heat-map arrays for constructing density layers based on coordinates and event counts; and timestamps for building dynamic visualisations. Y. Yu *et al.* (2025) highlighted that mobility dashboards benefit from multi-level drill-downs and explanations attached to visual primitives; indicator definitions and tooltips are therefore planned to be exposed that tie back to analytical computations. Y. Cao *et al.* (2025) demonstrated that heat-map overlays are effective for temporal crowding patterns, which motivates the inclusion of configurable time windows and colour scales for peak-hour exploration.

To align with digital-twin practices, B.P. Rafamatanantsoa *et al.* (2024) described City2Twin's separation of static 3D context from dynamic streams; the visual layer is planned to respect this separation by treating basemap and dynamic indicators as distinct sources, enabling smooth playback and reduced redraw overhead. H.A. Adrianto *et al.* (2024) showed that analyst-facing dashboards benefit from scenario toggles and multi-chart coordination; accordingly, the microservice is intended to provide filter panels (route, time, zone) that trigger coordinated updates across maps and charts. A. Wibowo *et al.* (2024) reported that disruption-aware overlays sourced from social streams shorten route-adjustment time in critical events; the design retains a pluggable "incident overlay" so that cities can add such feeds without altering the core renderer.

On the implementation side, the visualisation microservice is intended to be deployed as a separate front-end application that interacts with other system modules via a REST API. React is planned to be used as the primary technology, providing a component architecture with incremental UI updates. For web mapping, Leaflet or Mapbox GL JS are envisaged to serve as the cartographic engines; Leaflet offers lightweight vector overlays, while Mapbox GL enables GPU-accelerated styles and animated state transitions for moving objects. M. Laituri *et al.* (2025) drew attention to the value of real-time public dashboards during crisis response, and this is mirrored by reserving a "live mode" that prioritises update cadence and progressive rendering. For charts and heatmaps, Chart.js, D3.js, or Recharts are intended to be employed, with D3 reserved for bespoke interactions and Recharts for rapid composition in React. Where 3D context becomes a requirement, the microservice boundary is planned to admit a lightweight 3D scene (e.g., deck.gl) layered over the same data contracts to preserve consistency with 2D views.

In summary, the visualisation microservice is intended to provide a coherent, low-latency interface that turns complex spatio-temporal data into actionable views for diverse user groups. By standardising input contracts (GeoJSON, JSON tables, heat-map arrays) and separating map, chart, and filter concerns, the layer is expected to remain responsive under peak loads while preserving consistency of indicators across widgets. A focus on accessibility, progressive rendering, and clear affordances is intended to shorten time-to-insight for operational staff and to support reproducible analysis for experts. Through stateless rendering, cache-friendly assets, and explicit API boundaries, the microservice is positioned to scale independently of upstream analytics. Collectively, these properties are intended to ensure that the presentation tier strengthens decision-making without constraining future extensions such as 3D context or incident overlays.

Access and configuration management microservice. The access and configuration management microservice is intended to function as the administrative centre of the web-based traffic flow analysis system. Its primary aim is intended to be the provision of centralised control over

key system parameters and the offering of basic user authentication and authorisation capabilities. This is expected to enable the delineation of access levels to analytics, the configuration of data refresh frequency, and the adaptation of the system to the needs of a specific city or transport model. The functions of this microservice are proposed to include: creating and managing API keys required for integration with municipal or third-party data sources; setting integration parameters: city, route network, update timings, filters, and time intervals; defining user roles and managing access rights; maintaining an audit log to ensure transparency of administrative actions.

Implementing this microservice is intended to ensure the scalability and flexibility of the entire system without requiring modifications to the code of the core functional microservices. This is particularly important when deploying the system across multiple cities or under varying transport parameters and integration settings. The access and configuration management microservice is envisaged to perform a crucial systemic role – providing flexible administration of all key parameters of the web system and enforcing access restrictions for different user categories. Its functionality is divided into several core blocks:

1) API key management. The system is expected to provide an interface for creating, viewing, and deactivating API keys used to integrate municipal data sources. Each key can be associated with a specific subsystem (e.g., integration with GPS trackers or municipal portals) and constrained by expiry and request-rate limits.

2) Integration parameter configuration. An administrator is expected to be able to set core configuration parameters: city, set of transport routes, source polling cadence (e.g., every five minutes), time zone, and filters by transport type or city districts. These settings are intended to be stored centrally and propagated to other microservices via a configuration API.

3) Users and access roles. A basic authentication mechanism (e.g., tokens or JSON Web Token (JWT)) and role-based authorisation are provided. Typical roles are envisaged to be provided: administrator, analyst, and guest viewer. Each role is expected to grant access to a defined set of functions; for instance, only administrators are to be allowed to alter configuration or create API keys.

4) Audit log. All configurations are intended to be recorded with timestamp, author, and action type. This is expected to enable activity monitoring and to ensure transparency of system governance.

This microservice is not intended to process analytical or cartographic data; however, it is considered critical to the continuous operation of the entire system and to its adaptation to new conditions without code changes. Its presence is expected to render the system scalable, multi-scenario, and centrally manageable from a single point. The Access and Configuration Management microservice presupposes an administrative console through which authorised users are intended to be able to configure the system, create API keys, manage data refresh frequency, and define role-based access policies. Accordingly, the primary technological requirement is the rapid implementation of CRUD functions (Create, Read, Update, and Delete) with minimal front-end development effort.

Description of the overall architecture of the web-based traffic flow management system. The adoption of a microservice architecture is intended to enable the creation of a flexible and scalable transport system in which each component is expected to fulfil a narrowly specialised function. Z. Wang *et al.* (2025) reported that microservice decompositions support city-scale forecasting around metro stations, which aligns with the intention to keep compute hotspots independently scalable. C. Campos *et al*. (2025) argued that modelling data flows at the architectural level – within oneAPI-style pipelines – improves performance and manageability in multi-component systems; this view underpins the decision to foreground flow contracts between services. Integrating the diagrams and models within a single subsection is intended to ensure logical coherence and improves the perception of the architecture as a unified information space in which components are expected to operate in an interrelated and sequential manner.

At the architectural level, the system is envisaged to comprise the following principal containers:

- Frontend (client tier) – intended to provide users with access to transport-data visualisation, interactive charts, heatmaps, and configuration interfaces.
- API Gateway/Router – intended to coordinate user requests and to route them to the appropriate microservices.
- Microservices – Municipal API Integration, Data Processing and Aggregation, Analytics, Visualisation, and Access & Configuration Management – intended to encapsulate domain-specific responsibilities.
- Database – intended to serve as a central repository for aggregated and historical data.
- Configuration/Logging Store – intended to hold parameters, API keys, and audit logs.

Each microservice is intended to be deployed independently, allowing only those components under load to be scaled. The architectural style is intended to accord with contemporary approaches to mobility management systems – particularly in smart cities – where isolated logic, distributed data, and a high degree of modularity are preferred. Z. Wang *et al.* (2025) emphasised such modular scaling in urban mobility platforms, while C. Campos *et al.* (2025) highlighted coordination of heterogeneous compute stages via explicit flow specifications. Figure 4 presented the C4 container-level diagram of the system. The diagram is intended to present the overall architecture of the web-based traffic flow management system built on a microservice model. The system is described as consisting of several independent containers (microservices), each intended to perform a clearly defined function. The user (analyst, dispatcher, or operator) is expected to interact with the system via a React-based web interface. The web interface is intended to send requests to an API Gateway, which

is intended to act as a router between the client and the internal microservices. All processed information is intended to be stored in a central database (PostgreSQL), while configuration parameters – including change logs and tokens – are intended to be maintained in a separate configuration store (Redis or JSON-based storage). Beyond the structural architecture and user scenarios, an important aspect of conceptual modelling is intended to be the description of how data are transmitted and transformed within the system. For this purpose, a DFD is planned to be employed to depict, in a clear and intuitive manner, the sources, processors, stores, and directions of information flow.

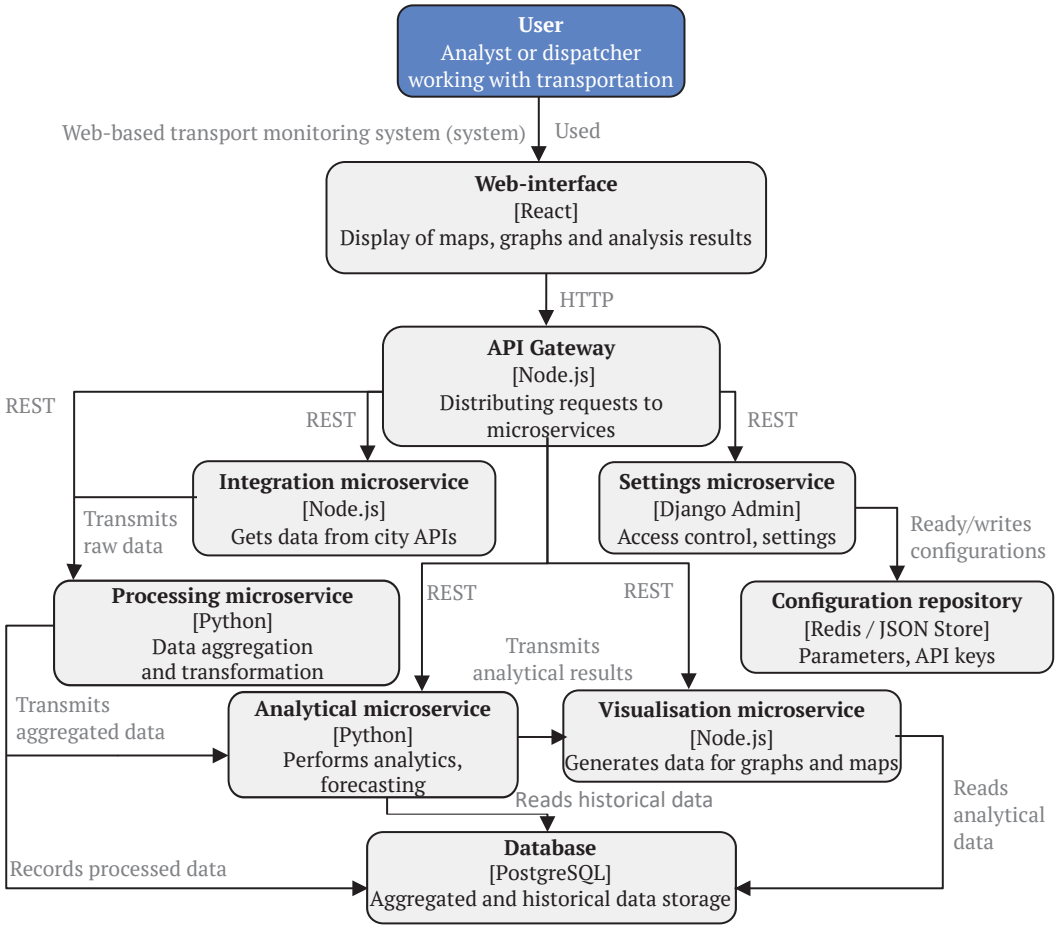

***Figure 4**. C4 container-level diagram*

***Source:** designed by the authors*

Such diagrams were particularly valuable in transport information systems where large volumes of real-time streams require structured processing; this observation supports the choice to make data-flow boundaries explicit. B.P. Rafamatanantsoa *et al.* (2024) showed, in the City2Twin context, that microservice-oriented architectures facilitate the tracing and scaling of data flows across dynamic streams and static context; the DFD is intended to mirror this separation of concerns. The components captured by a DFD are intended to include: external data sources/receivers (users, APIs); processing processes (microservices); intermediate and final data stores (database, cache); data flows between components. The DFD for the traffic flow management system is intended to be shown in Figure 5. The data-flow diagram is intended to depict the key information transformations within the system. Data are expected to arrive from external sources (municipal APIs), to be processed by the integration and aggregation microservices, to be stored in the database, to be subjected to analytical processing, and ultimately to be presented to the user. All processes are intended to be configured via a dedicated configuration microservice, which is expected to ensure flexibility, centralised parameter control, and efficient data movement. For the storage, processing, and subsequent analysis of transport data, the web system is intended to employ a centralised relational database. Its structure is intended to be modelled using an ER diagram, which is intended to visualise the core entities, their attributes, and the relationships between them. S. Batita *et al.* (2024) reported that relational, domain-oriented schemas remain effective in urban transport systems for scalability and analytical integration, while A. Mansurova *et al.* (2025) described schema designs that handle high-volume GPS

events under city workloads; these findings motivate the choice of a relational backbone with explicit keys and constraints. The list of database entities is intended to be presented in Table 2.

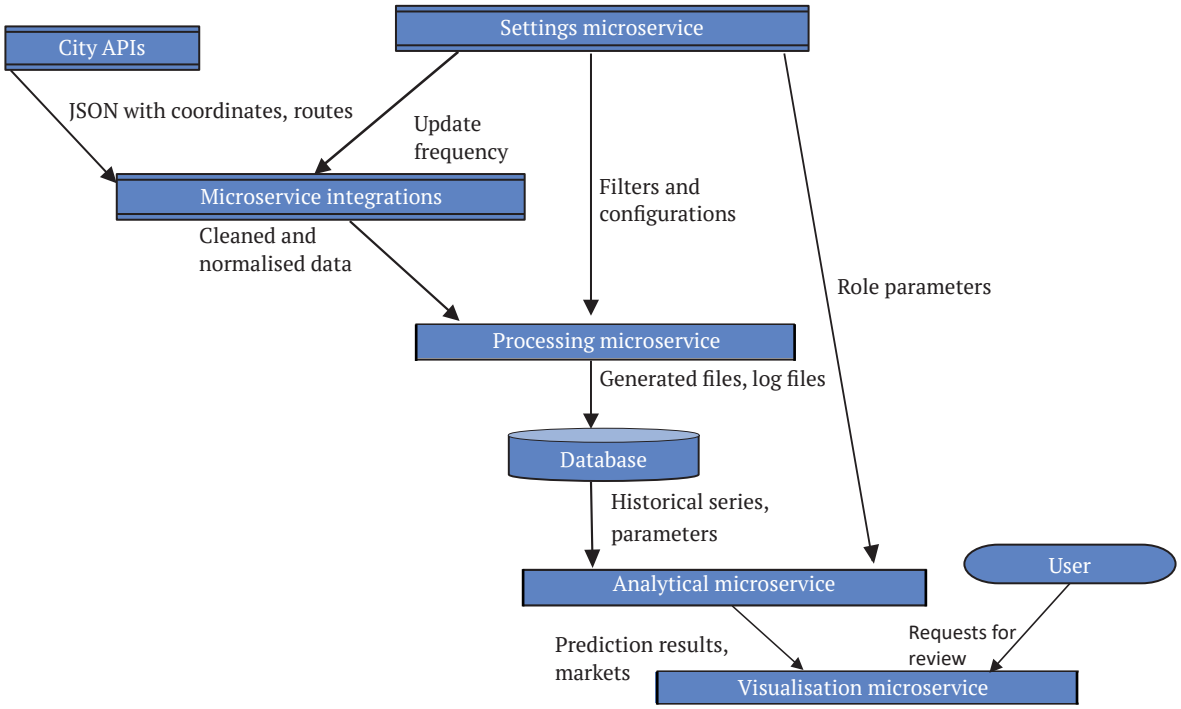

***Figure 5**. Service DFD diagram*

***Source:** designed by the authors*

***Table 2**. Principal database entities*

Entity	Description
Routes	Route number, mode of transport, origin and terminus stops.
Vehicles	Identifier, type, associated route number, GPS coordinates.
Stops	Stop name, coordinates, list of routes serving the stop.
Traffic events	Timestamp, location, delay, vehicle ID, distance to the nearest stop.
Analytics/Forecast	Model type, route ID, date, forecast output.
Users	Name, role (analyst, administrator), access token.

***Source:** compiled by the authors*

Figure 6 presented a visual representation of the database in the form of an ER diagram. It is intended to outline the core entity sets (such as Routes, Vehicles, Stops, MovementEvents, Indicators, Users/Roles, and Configurations) together with their primary-foreign key relationships and cardinalities. The diagram is expected to guide normalisation choices (for example, separating time-stamped movement events from relatively static vehicle or route metadata) and to make integrity constraints explicit for implementation. By fixing these invariants at the schema level, the model is positioned to support scalable ingestion, consistent historical queries, and reproducible analytics across different city deployments. The ER diagram is intended to depict the structure of the database that is expected to store information on transport routes, vehicles, stops, traffic events, and analytical results. Each route is intended to be linked to a set of vehicles and stops; each vehicle is intended to be associated with movement events; and each analytical record is intended to be generated by a system user. This model is intended to encode relationships between real-world objects and to support rapid access to the required information. In summary, the overall architecture is intended to provide a clear separation of concerns, where each microservice fulfils a narrowly scoped role and communicates through explicit, well-typed contracts. This decomposition is expected to simplify scaling and fault isolation, while the API Gateway, shared schemas, and configuration store maintain coherence across the system. The C4, DFD, and ER artefacts together are meant to anchor implementation and testing by fixing boundaries, data flows, and invariants before code. Operationally, the design aims to balance near-real-time updates with batch consolidation, so that cities can tune latency, load, and cost to local needs. Collectively, these properties are intended to deliver a robust foundation for deployment, evolution, and reproducible analysis in heterogeneous urban environments.

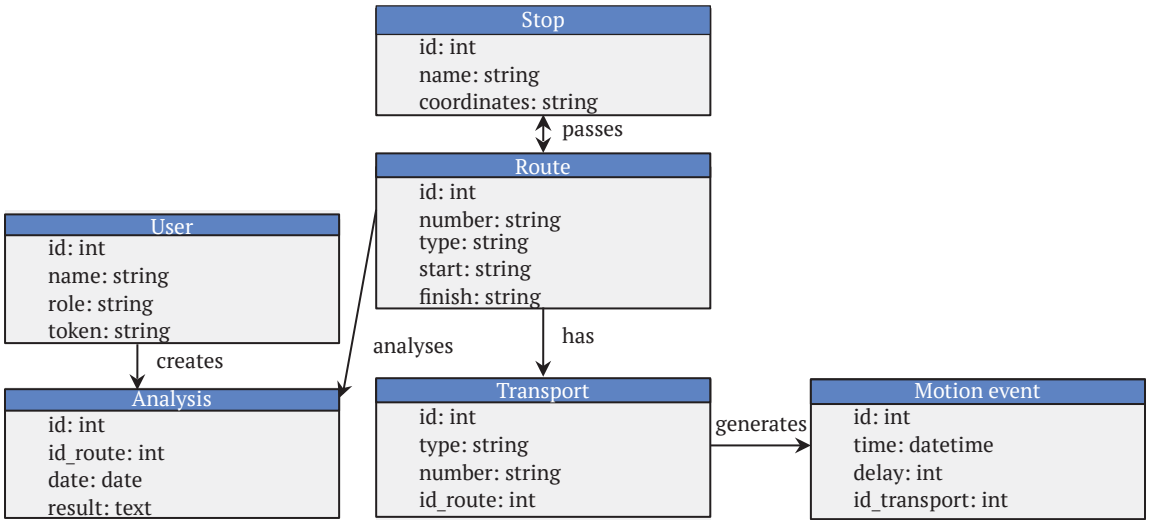

***Figure 6**. ER diagrams of the databases*

***Source:** designed by the authors*

Conclusions

The study has enabled the formulation of a coherent conceptual model of a web-based system for managing urban traffic flows grounded in a microservice architecture. It was found that delineating the system's functional zones at the microservice level ensures a clear separation of responsibilities and facilitates scaling without disrupting the overall data-processing logic. The analysis showed that the chosen sequence of modelling artefacts – an ER diagram for the domain, a multi-level DFD to trace information flows, and a C4 diagram to refine container boundaries and interactions – is sufficient for the unambiguous reproduction of the proposed architecture by other researchers and developers. It was demonstrated that integrating these artefacts within a single methodological framework minimises ambiguities in data interpretation and conflicts between components, which is particularly important in urban scenarios characterised by heterogeneous data sources.

It was found that the asynchronous interaction of the integration module with municipal application programming interfaces ensures stable message intake and simplifies the unification of data formats. The analysis showed that deploying a dedicated processing and aggregation module makes it possible to standardise core traffic metrics and prepare aligned temporal slices for subsequent interpretation. It was substantiated that the analytics module should be constructed as a superstructure over aggregated indicator sets, focusing on the computation of indicators and baseline forecasts, whereas the visualisation microservice provides cartographic and time-series renderings of results for the prompt interpretation of situations across the urban space.

The proposed separation of processing into operational and periodic modes proved methodologically sound. It was established that the operational loop is appropriate for obtaining current indicators of load and deviations from the timetable, whereas the periodic loop serves to reconcile historical data and to construct aggregate measures. It was demonstrated that unified metric definitions and deterministic calculation functions are critical to the reproducibility of results across diverse urban contexts and ensure consistency between visual representations and the outputs of the analytics module. Future research will focus on the stepwise validation of the model using real urban data, the deployment of a prototype connected to open application programming interfaces, the extension of the analytics module with methods for forecasting short-term delays and overloads, and the development of harmonised visualisation scenarios for different user categories, thereby enabling an assessment of the proposed architecture's scalability and reproducibility under practical conditions.

Acknowledgements

The authors express their gratitude to the State University of Trade and Economics, which provided comprehensive support for scientific research by university teachers and postgraduate students.

Funding

None.

Conflict of Interest

None.

References

[1] Adrianto, H.A., Sitanggang, I.S., Akbar, A., Neyman, S.N., & Azhim, M.F. (2024). Interactive dashboard for visualization and analysis of landcover change and land/forest fire. *IOP Conference Series: Earth and Environmental Science*, 1418, article number 012082. doi: 10.1088/1755-1315/1418/1/012082.

[2] Barabash, O., Weigang, G., & Komar, K. (2021). Formation of traffic safety profile in central parts of the city and its informational protection. *Transport Technologies*, 2(2), 42-51. doi: 10.23939/tt2021.02.042.
[3] Batita, S., Makni, A., & Amous, I. (2024). Intelligent transportation systems: A survey on data engineering. In *DATA 2024 proceedings of the 13th international conference on data science, technology and applications* (pp. 169-179). Setúbal: SCITEPRESS – Science and Technology Publications. doi: 10.5220/0012857300003756.
[4] Beeraka, B.S. (2025). Enterprise microservices: Revolutionizing telecom network architecture. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 11(1), 290-297. doi: 10.32628/cseit25111231.
[5] Bokolo, A. (2025). Enabling seamless interoperability of digital systems in smart cities using API: A systematic literature review. *Journal of Urban Technology*, 31(4-5), 123-156. doi: 10.1080/10630732.2024.2427543.
[6] Campos, C., Asenjo, R., & Navarro, Á. (2025). Exploring data flow design and vectorization with oneAPI for streaming applications on CPU+GPU. *The Journal of Supercomputing*, 81, article number 428. doi: 10.1007/s11227-024-06891-3.
[7] Cao, Y., Li, Q.-J., & Yang, Z. (2025). Identifying the spatial range of the Pearl River Delta urban agglomeration from a differentiated perspective of population distribution and population mobility. *Applied Sciences*, 15(2), article number 945. doi: 10.3390/app15020945.
[8] Danyliuk, A., & Muliarevych, O. (2024). Ant colony algorithm in traffic flow control. *Advances in Cyber-Physical Systems*, 9(2), 158-163. doi: 10.23939/acps2024.02.158.
[9] Erişkin, E. (2024). Collaborative game-theoretic optimization of public transport fare policies: A global framework for sustainable urban mobility. *Sustainability*, 16(24), article number 11199. doi: 10.3390/su162411199.
[10] Fornalchyk, Y., & Hilevych, V. (2023). Characteristics of motorization's impact on the urban population. *Transport Technologies*, 4(2), 68-75. doi: 10.23939/tt2023.02.068.
[11] Horokhovskyi, O., & Oshovska, K. (2015). Quality management and obtaining optimal results in the city's transport network management system. *Information Technologies and Computer Engineering*, 12(3), 29-32.
[12] Inamdar, S.A., & Kulkarni, S.S. (2025). Advancing traffic volume prediction and synthetic data generation with machine learning and deep learning. *International Journal for Multidisciplinary Research*, 7(1), 1-18. doi: 10.36948/ijfmr.2025.v07i01.35530.
[13] Kotenko, M., Moskalyk, D., Kovach, V., & Osadchyi, V. (2024). Navigating the challenges and best practices in securing microservices architecture. In *CPITS-II 2024: Workshop on cybersecurity providing in information and telecommunication systems II* (pp. 1-16). Kyiv: Borys Grinchenko Kyiv Metropolitan University.
[14] Kozachenko, D.M., Klyga, O.V., & Kharchenko, Ye.V. (2025). Modeling of train sets in tasks of railway stations technical and operational evaluation. *Science and Transport Progress*, 2(110), 88-97. doi: 10.15802/stp2025/331674.
[15] Laituri, M., Kalra, Y., & Yang, C. (2025). The disappearance of COVID-19 data dashboards: The case of ephemeral data. *COVID*, 5(1), article number 12. doi: 10.3390/covid5010012.
[16] Leghemo, I.M., Segun-Falade, O.D., Odionu, C.S., & Azubuike, C. (2025). Continuous data quality improvement in enterprise data governance: A model for best practices and implementation. *Journal of Engineering Research and Reports*, 27(2), 29-45. doi: 10.9734/jerr/2025/v27i21391.
[17] Mansurova, A., Mussina, A., Aubakirov, S., Nugumanova, A., & Yedilkhan, D. (2025). From raw GPS to GTFS: A real-world open dataset for bus travel time prediction. *Data*, 10(8), article number 119. doi: 10.3390/data10080119.
[18] Matseliukh, Y., & Lytvyn, V. (2024). Modeling of passenger flows analysis system of low-carbon transportation in a smart city. *Information Systems and Networks*, 15, 430-448. doi: 10.23939/sisn2024.15.430.
[19] Ntouros, K., Papatheodorou, K., Gkologkinas, G., & Drimzakas-Papadopoulos, V. (2025). A Python framework for crop yield estimation using Sentinel-2 satellite data. *Earth*, 6(1), article number 15. doi: 10.3390/earth6010015.
[20] Ohonovskyi, Y., Berko, A., Chyrun, L., & Chyrun, S. (2023). Information system prototype for monitoring and content analysis of complaints from smart city residents. *Information Systems and Networks*, 13, 24-45. doi: 10.23939/sisn2023.13.024.
[21] Oyenuga, A.O., Apeh, C.E., Odionu, C.S., & Austin-Gabriel, B. (2025). Advancing public safety and housing solutions: A comprehensive framework for machine learning and predictive analytics in urban policy optimization. *International Journal of Frontiers in Science and Technology Research*, 8(1), 24-43. doi: 10.53294/ijfstr.2025.8.1.0024.
[22] Power BI Community. (2021). Power BI challenge 12 wrap up: Transport & shipping data. *Microsoft Power BI Community Blog*. Retrieved from https://community.powerbi.com/t5/Community-Blog/Power-BI-Challenge-12-Wrap-Up-Transport-amp-Shipping-Data/ba-p/1788343.
[23] Puzio, E., Drozdz, W., & Kolon, M. (2025). The role of intelligent transport systems and smart technologies in urban traffic management in Polish smart cities. *Energies*, 18(10), article number 2580. doi: 10.3390/en18102580.
[24] Quesado Filho, N.O., Guimarães, C.G.C., & Oliveira-Neto, F.M. (2025). Gtfswizard: A set of tools for exploring and manipulating general transit feed specification in R language. *Contribuciones a Las Ciencias Sociales*, 18(1), article number e14620. doi: 10.55905/revconv.18n.1-197.

[25] Rafamatanantsoa, B.P., Jeddoub, I., Yarroudh, A., Hajji, R., & Billen, R. (2024). City2Twin: An open urban digital twin from data integration to visualization and analysis. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 48(2), 387-394 doi: 10.5194/isprs-archives-xlviii-2-w8-2024-387-2024.
[26] Şahin, G., Avcı, D.A., Karagenç, Ş., Pak, B.K., Seke, P., & Tunalı, A.Ç. (2024). Enhancing user experience in insurance applications: Adopting microservices architecture and innovative methods. *Orclever Proceedings of Research and Development*, 5(1), 274-284. doi: 10.56038/oprd.v5i1.548.
[27] Schetakis, N., Bonfini, P., Alisoltani, N., Blazakis, K., Tsintzos, S.I., Askitopoulos, A., Aghamalyan, D., Fafoutellis, P., & Vlahogianni, E.I. (2025). Data re-uploading in Quantum Machine Learning for time series: Application to traffic forecasting. *arXiv*. doi: 10.48550/arXiv.2501.12776.
[28] Volkov, D., & Liubchenko, V. (2024). Securing microservices: Challenges and best practices. In *ICST-2024 information control systems & technologies*. Odesa: Odesa Polytechnic National University.
[29] Wang, Z., Yu, D., Zheng, X., Meng, F., & Wu, X. (2025). A model-data dual-driven approach for predicting shared bike flow near metro stations. *Sustainability*, 17(3), article number 1032. doi: 10.3390/su17031032.
[30] Wibowo, A., Ruslanjari, D., Surahmat, A., Karyaningsih, D., & Vera, N. (2024). The MxT model: Leveraging social media data for real-time route optimization in disaster-prone urban transport networks. *International Journal of Transport Development and Integration*, 8(4), 587-594. doi: 10.18280/ijtdi.080410.
[31] Yang, F. (2025). Leveraging mobile interaction technologies for real-time decision making in enterprise management systems. *International Journal of Interactive Mobile Technologies*, 19(2), 65-78. doi: 10.3991/ijim.v19i02.53743.
[32] Yu, Y., Wang, Y., Zhang, Y., Qu, H., & Liu, D. (2025). InclusiViz: Visual analytics of human mobility data for understanding and mitigating urban segregation. *arXiv*. doi: 10.48550/arXiv.2501.03594.

Концептуальна модель веб-системи управління транспортними потоками у міському середовищі на основі мікросервісної архітектури

Андрій Роскладка
Доктор економічних наук, професор
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0000-0002-1297-377X
Євгеній Пострелко
Аспірант
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0000-0001-9730-450X

Анотація. Актуальність дослідження зумовлена зростанням навантаження на міську транспортну інфраструктуру, потребою у цифровій трансформації управління мобільністю та впровадженні інтелектуальних технологій аналізу даних у режимі реального часу. Така система дає змогу оперативно реагувати на зміни у русі транспорту, підвищувати ефективність маршрутної мережі та покращувати якість міських перевезень. Метою дослідження було формування архітектури веб-системи, яка забезпечує інтеграцію даних із міських інтерфейсів прикладного програмування, їх автоматизовану обробку, аналітичну інтерпретацію, візуалізацію результатів та централізоване керування конфігураціями. Методологічну основу становили підходи системного аналізу, моделювання потоків даних, побудова діаграм «сутність-зв'язок» та застосування архітектурних шаблонів для відображення структурної та функціональної взаємодії компонентів. У статті розроблено концептуальну модель веб-системи управління транспортними потоками у міському середовищі, побудовану за принципами мікросервісної архітектури. Результатом роботи було створення структурної моделі системи, що включила п'ять взаємопов'язаних мікросервісів: інтеграції з міськими інтерфейсами прикладного програмування (Node.js), обробки та агрегації даних (Python, Redis Streams), аналітичного модуля з підтримкою алгоритмів машинного навчання (Scikit-learn), модуля візуалізації (React, Mapbox, Chart.js) та сервісу керування доступом і конфігураціями. Детально описано логіку їхньої взаємодії, механізми масштабування та забезпечення відмовостійкості. Практична цінність дослідження полягала у розробленні універсальної архітектонічної основи для впровадження систем аналітики й моніторингу міського транспорту, що можуть стати прототипом інтелектуальних платформ управління мобільністю в концепції Smart City

Ключові слова: розподілені інформаційні сервіси; цифрове моделювання міської мобільності; аналіз потоків даних у реальному часі; веб-аналітика транспортних систем; візуалізація просторово-часових даних; Smart City

TECHNOLOGIES AND ENGINEERING

Journal homepage: https://technologies-engineering.com.ua/en
Vol. 26, No. 4, 2025

Received: 23.04.2025
Revised: 19.08.2025
Accepted: 17.09.2025

UDC 615.32:615.9:615.37

DOI: 10.30857/2786-5371.2025.4.6

Development of the composition and technology of an alcohol-free hand sanitiser

Hanna Tarasenko*
PhD in Technical Sciences, Associate Professor
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-0995-7322
Olena Saliy
PhD in Pharmacy, Associate Professor
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
https://orcid.org/0000-0001-7103-2083
Bohdan Muravskyi
Master
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
https://orcid.org/0009-0009-6511-8222
Maria Popova
Postgraduate Student
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-2579-0331
Galyna Kuzmina
PhD in Chemical Sciences, Associate Professor
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-0691-8563

Abstract. Effective hand hygiene is a key factor in the prevention of infectious diseases, which creates a need for safe and highly effective antiseptic products and underscores the relevance of developing formulations with optimal antimicrobial, dermatological, and technological properties. The objective of the study was to develop an alcohol-free hand antiseptic with high antimicrobial activity, skin safety, and compatibility with sensor-based dispensers. The analysis of the hand antiseptic market was conducted using analytical and statistical methods, while the determination of quality parameters of the hand antiseptic was carried out using organoleptic, physicochemical, and microbiological control methods. It was established that alcohol-based products – ethanol, propanol, and isopropanol – dominate the antiseptic market (over 70%), and their main limitations were identified, including the potential to cause skin dryness, risk of irritation with prolonged use, and increased flammability. Based on the conducted analysis, an alcohol-free composition was proposed, in which benzalkonium chloride (0.1-0.15%) was identified as the optimal active ingredient. Four formulation variants with different essential oils were studied; it was determined that the samples had a pH ranging from 4.8 to 5.3 and a viscosity of 22-24 mPa·s. The sample containing demonstrated the best overall parameters, with a pH of 5.3 ± 0.2, viscosity of 23 ± 0.3 mPa·s, transparency and stability, as well as improved organoleptic properties. All samples met microbiological requirements, and the content of benzalkonium chloride was 0.12 ± 0.02%, confirming accurate dosing. A technological process for obtaining the antiseptic through the preparation of two phases followed by

Suggested Citation:
Tarasenko, H., Saliy, O., Muravskyi, B., Popova, M., & Kuzmina, G. (2025). Development of the composition and technology of an alcohol-free hand sanitiser. *Technologies and Engineering,* 26(4), 68-76. doi: 10.30857/2786-5371.2025.4.6.

*Corresponding author

their combination was proposed, ensuring the stability and homogeneity of the final product. The results of this study can be utilised by manufacturers of cosmetic and disinfectant products to create alcohol-free hand antiseptics suitable for use in medical, educational, and social institutions, as well as in household settings, including applications with sensor-based hand sanitiser dispensers

Keywords: hygienic agent; benzalkonium chloride; essential oil; dissolution; hand hygiene; sensor dispenser

Introduction

There is a growing trend toward the replacement of alcohol-based antiseptics with products containing natural-origin components. Increasingly, formulations include essential oils (tea tree, eucalyptus, lavender), plant extracts (chamomile, calendula, green tea), and biopolymers (hyaluronic acid, aloe vera). These substances provide mild antimicrobial activity and contribute to the preservation of the natural skin microbiome, which aligns with the modern concept of "skin microbiome-friendly cosmetics". Accordingly, alcohol-free antiseptics are becoming particularly relevant when combined with sensor-based dispensers, which ensure contactless application and significantly reduce the risk of cross-contamination. The development of an effective alcohol-free product allows for the combination of pronounced antimicrobial activity with skin safety and user comfort, which is important both for healthcare facilities and for public spaces, offices, and educational institutions.

Alcohol-based hand sanitisers (ABHS) have become especially valued for their fast-acting properties, versatility, and proven effectiveness in reducing microbial and viral loads in hands. C. Villa & E. Russo (2021) reported that the essential formulation components of ABHS comprise an alcohol base, typically ethanol or propanol, combined with water, supplemented with minor quantities of hydrogen peroxide and glycerin. These constituents collectively contribute to the sanitiser's antimicrobial effectiveness while maintaining skin tolerability. However, the standard formulation has certain limitations related to its delivery and distribution properties, which has prompted the inclusion of thickeners to prevent leakage and improve overall efficacy. O. Atolani *et al.* (2020) emphasised that the main consumer-level safety concerns associated with alcohol-based hand antiseptics include their flammability, accidental or intentional ingestion, and potential adverse local effects. The study by S. Dalasile *et al.* (2024) confirmed that ethanol from disinfectants can cause intoxication, hypoglycemia, and impaired consciousness. In addition to toxicological risks, such products were characterised by increased fire hazard due to volatile alcohol vapors, which create a risk of ignition when exposed to open flame or heat sources. D. Gupta & A. More (2021) reported cases of skin burns among staff due to non-compliance with safety measures. Dermatological complications (dryness, irritation, contact dermatitis) are typically listed separately in the "Contraindications" section, which is especially important when alcohol concentration is high or the product is used improperly. A. Rafizadeh *et al*. (2023) demonstrated the presence of substandard alcohol-based hand hygiene products on the market, revealing insufficient alcohol concentrations (<60%) and the occurrence of unacceptable toxic contaminants, including methanol, which compromises both antiseptic efficacy and consumer safety.

To enhance consumer properties, dermatological safety, and efficacy of hand antiseptics, in addition to alcohol, excipients may be included in their composition, such as humectants, gelling agents, fragrances, as well as plant extracts or silver nanoparticles (Perveen *et al.,* 2024). K. Abuga & N. Nyamweya (2021) also emphasised the importance of considering various formulation factors, including the type and concentration of alcohol, as well as inactive ingredients, when determining the overall efficacy and safety of alcohol-based hand sanitisers. The study T. Saha *et al.* (2021) highlighted that, alongside the high demand for ABHS, significant challenges emerged regarding formulation standardisation and safety. The authors reported risks associated with improper use, including burns and toxic reactions, emphasising the need for effective labeling and regulatory control to minimise consumer harm. These findings underscored the importance of ensuring both efficacy and safety in ABHS. The research O.V. Pokryshko & T.I. Pyatkovskyy (2025) demonstrated that ethanol-based formulations exhibited higher antimicrobial activity compared to isopropanol-based products. However, the study also revealed the presence of ineffective or contaminated products on the market, highlighting the urgent need for strengthened regulatory oversight and quality assurance in Ukraine. These results emphasised the variability of product quality and the importance of monitoring local markets. Innovations in ABHS formulation have been explored by L. Večerková *et al.* (2024), who proposed a novel powdered hand sanitiser with controlled release of active ingredients. This approach may reduce the frequency of reapplication and potentially decrease skin irritation associated with conventional alcohol gels. The study illustrated a promising direction for improving consumer compliance, safety, and overall product performance.

Research into the development of hand antiseptics has highlighted the importance of balancing high antimicrobial efficacy, user safety and innovative formulation strategies. Although alcohol-based products are effective, their limitations, such as skin irritation and unsuitability for sensitive populations, have highlighted the need to find alternative solutions. In response to these issues, the present study aimed to develop an alcohol-free antiseptic formulation that provides robust antimicrobial activity, ensures safety and tolerability, and is compatible with sensor dispenser systems.

Materials and Methods

The analysis of the hand antiseptic market was conducted using a set of analytical and statistical methods aimed at achieving a comprehensive and objective characterisation of its structural features. The study relied on data retrieved from the State Register of Disinfectants (Resolution of the Cabinet of Ministers of Ukraine No. 863, 2023), which served as a reliable and authoritative source for assessing the current market environment. Analysis of the disinfectants register data allowed for the assessment of the current state of the disinfectants market, its diversity in terms of composition and intended use, and underscores the importance of state control over product quality and safety. The analytical framework included the following criteria: systematic classification of products according to the chemical nature of their active ingredients; differentiation of antiseptics by their intended use; examination of dosage forms and technological characteristics; and statistical assessment of the proportional distribution of products across the identified categories. Formulation optimisation was carried out by varying the concentrations of active ingredients and excipients to achieve the desired viscosity, stability, and uniform distribution of the active components, thereby ensuring high antimicrobial efficacy and dermatological safety of the developed antiseptic. Table 1 presented the composition of the developed alcohol-free hand antiseptic, along with the functional purpose and mechanism of action of each component.

***Table 1**. Composition and functional purpose of components in the alcohol-free hand antiseptic*

Component	Content (mass %)	Function	Mechanism of action	Justification for inclusion in the formula
Benzalkonium Chloride (Merck KGaA, Germany)	0.1-0.15	Antimicrobial agent.	Disrupts bacterial membranes and viral envelopes, causing microbial death.	Effective against Gram-positive and Gram-negative bacteria and enveloped viruses; allows safe use without alcohol.
Cocamidopropyl PGDimonium Chloride Phosphate (M.C. Biotec Inc., China)	1.0-3.0	Gentle skin cleansing; improves product distribution.	Reduces surface tension, ensures uniform application of antimicrobial components.	Amphoteric surfactant that minimises irritation, improves cosmetic properties and efficacy of the antiseptic.
Propylene glycol (Hedinger GmbH, Germany)	3.0-6.0	Humectant; improves glide.	Retains water in the upper layers of the skin; reduces formula viscosity.	Moisturising component that supports skin hydration and compatibility with sensor dispensers.
Triethylene Glycol (Dow Chemical Company, USA)	1.0-2.0	Additional antimicrobial agent; stabiliser.	Suppresses growth of bacteria and viruses; reduces evaporation of active components.	Enhances formula stability and the effectiveness of the alcohol-free antiseptic.
Polysorbate20 (CDH Fine Chemical, India)	0.2-0.5	Emulsifier; aroma stabilisation.	Forms stable colloidal systems, prevents phase separation.	Ensures organoleptic stability and no adverse impact on antimicrobial activity.
Essential oils of *Citrus limon* (HBNO® Bulk Essential Oils, Germany), *Citrus sinensis* (Isope Provence, France), *Lavandula angustifolia* (Visagenics, Bulgaria), and *Melaleuca alternifolia* (NatureInBottle, India)	0.01-0.08	Fragrancer; antiseptic and antiinflammatory action.	Disrupts membranes of bacteria and viral envelopes; enhances skin barrier function.	Boosts antiseptic activity, improves organoleptic properties of the solution.
Water	up to 100	Main solvent; provides liquid consistency.	Dissolves the active components and ensures uniform application on skin.	Ensures physicochemical stability and correct concentration of active components.

***Source:** developed by the authors of this study*

The technological process for the production of the antiseptic involved the preparation of two phases – an aqueous phase and an antimicrobial phase – in two separate reactors. In the first reactor, at a temperature of 25-30°C, the aqueous phase was prepared by dissolving Cocamidopropyl PG-Dimonium Chloride Phosphate in purified water obtained by reverse osmosis. This component reduced surface tension and ensured uniform distribution of the antimicrobial ingredients. Propylene glycol was then added as a humectant, and triethylene glycol was incorporated as an additional antimicrobial agent and stabiliser. Simultaneously, in the second reactor, benzalkonium chloride was dissolved in purified water at 25-30°C to reduce system viscosity and facilitate dissolution of the active ingredient, while maintaining solution homogeneity within a pH range of 4.5-6.0. After stabilising both phases, they were combined under moderate stirring to obtain a homogeneous, transparent solution. Essential oils (*Citrus limon*, *Citrus sinensis*, *Lavandula angustifolia*, *Melaleuca alternifolia*), previously dissolved in a small amount of Polysorbate-20

to ensure colloidal stability and uniform distribution of the antiseptic and aromatic components, were then added.

The final solution was filtered through a membrane (0.45-1 μm) to remove mechanical impurities and subsequently filled into bottles. After bottling, organoleptic evaluation and assessment of the physicochemical parameters of the product were conducted according to the quality specifications for the finished product. To evaluate the influence of essential oils on the quality of the alcohol-free antiseptic solution, four variants were prepared with active components: Benzalkonium Chloride (0.1-0.15%) and essential oils of *Citrus limon* (Sample 1), *Citrus sinensis* (Sample 2), *Lavandula angustifolia* (Sample 3), and *Melaleuca alternifolia* (Sample 4). The pH was determined using a 949 pH Meter (Metrohm, Switzerland). Measurements were carried out within a controlled temperature range of 23-25°C, which was maintained throughout the entire experiment. The viscosity was measured using a DVPlus-II viscometer (Brookfield, USA).

Results and Discussion

During state registration with the authorised regulatory authorities, difficulties may arise in correctly determining the legal status of products labelled as "antiseptic" or "antibacterial". Such products may fall under various regulatory categories – biocidal products, cosmetic products, medicinal products, or medical devices – depending on their declared purpose and functional characteristics. The distinction between cosmetic products and medicinal products is particularly debatable, as classification is determined by the therapeutic intent of the product. According to the recommendations of the Oder of the Ministry of Health of Ukraine No. 1247 (2024), if a product claims therapeutic or prophylactic properties against infectious processes or skin lesions, it is most likely regulated as a medicinal product. In certain cases, such products may also be subject to regulation under the Technical Regulation on Medical Devices (Resolution of the Cabinet of Ministers of Ukraine No. 753, 2013).

Based on an analysis of available sources and official data, it was established that, as of September 11, 2025, approximately 1,130 Ukrainian and imported products are registered in the State Register of Disinfectants (Ministry of Health of Ukraine, 2025). These products have either received state registration or undergone re-registration following the examination of registration materials conducted by the expert institution – the State Enterprise "Committee on Hygienic Regulation of the Ministry of Health of Ukraine". The data analysis revealed that, among all registered disinfectants, only 37 products (3.27%) are intended for prophylactic disinfection and decontamination of personnel hands in healthcare, educational, child-care, sports, social, and penitentiary facilities, military units, enterprises of various industries, and establishments in the hospitality, retail, entertainment sectors, and communal services. These products were presented in Figure 1, which illustrated the distribution of various types of hand disinfectants in the market.

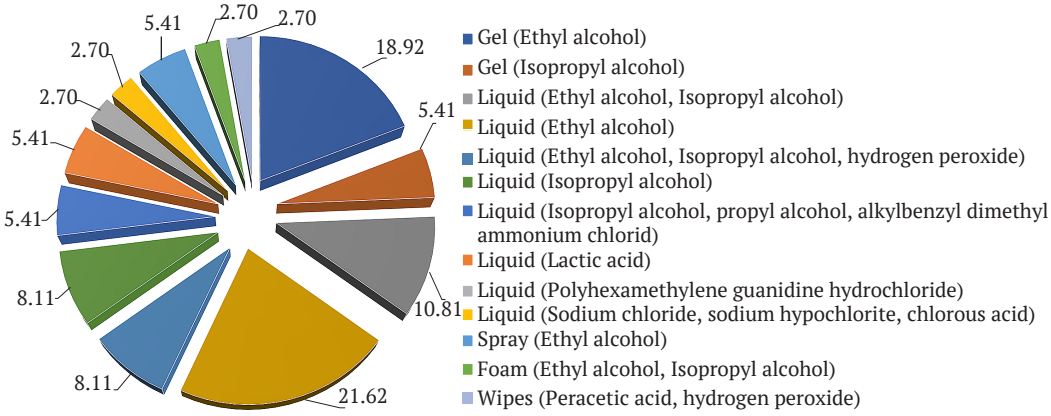

***Figure 1**. Products for preventive hand disinfection and decontamination (%)*
***Source:** developed by the authors of this study*

The pie chart illustrated the distribution of different types of hand disinfectants available in the market. The largest share is occupied by liquid formulations containing ethyl chloride, sodium hypochlorite, or chlorous acid, accounting for 21.62% of the total. This is followed by gel formulations with ethyl alcohol (18.92%) and liquid formulations containing a combination of ethyl alcohol and isopropyl alcohol (10.81%). Smaller portions are represented by foams containing ethyl and isopropyl alcohol (8.11%), sprays with ethyl alcohol (8.11%), and liquids with isopropyl alcohol alone (5.41%). Other minor categories, each comprising between 2.70% and 5.41%, include gels with isopropyl alcohol, liquids with ethyl alcohol only, liquids with a combination of ethyl alcohol, isopropyl alcohol, and hydrogen peroxide, liquids with isopropyl alcohol and propyl alcohol plus alkylbenzyl dimethyl ammonium chloride, liquids with polyhexamethylene guanidine hydrochloride, and wipes containing peracetic acid and hydrogen peroxide. Overall, the chart highlighted that alcohol-based gels and liquids dominate the disinfectant market, with

alternative forms such as sprays, foams, and wipes representing smaller segments.

It was established that the Ukrainian retail pharmacy and supermarket sectors feature a segment of compact, pocket-sized hand antiseptics (Table 2), produced by Ukrainian pharmaceutical and cosmetic companies. These products combine high antimicrobial efficacy with dermatological safety and ease of use due to their compact bottle design. The antiseptics are intended not only to eliminate pathogenic microorganisms but also to support the natural barrier functions of the skin. A comparison of the formulations revealed that these products contain moisturising, emollient, and antioxidant components such as glycerin, panthenol, aloe vera, and vitamin E. The inclusion of these ingredients minimises the risk of dryness, irritation, and allergic reactions, ensuring comfortable and prolonged use of the products in both domestic and professional settings. By supporting the barrier functions of the skin, these formulations reduce the risk of skin dryness, irritation, and hypersensitivity, providing a comfortable and safe experience for extended use in everyday and occupational environments.

***Table 2**. Hand antiseptics in the Ukrainian retail pharmacy and supermarket*

Manufacturer / Country	Name	Form	Composition
LLC "Medical Scientific and Production Association BIOKON", Ukraine	Antiseptic Hand Spray "Aloe Vera and Sage"	Spray	Isopropanol (70%), water, aloe vera extract, sage oil, tea tree oil.
	Antiseptic Hand Gel	Gel	Isopropanol, water, PEG 8, DEC, triclocarban, bisabolol, panthenol, fragrance composition.
LLC Lysoform Medical, Ukraine	Hand / Skin Antiseptics	Gel / Liquid	Mixture of isopropyl alcohol and 1-propanol (>70%).
LLC LekoPro, Ukraine	Hand Antiseptic Spray "Chlorhexidine Bigluconate 0.05%"	Spray	Purified water, chlorhexidine bigluconate 0.05%.
	Antiseptic Lotion	Liquid	Isopropyl alcohol, water, glycerin, benzalkonium chloride, benzyl alcohol, benzyl salicylate, fragrance.
LLC "UNIKS", Ukraine	Universal Antiseptic Spray for Hands / Surfaces	Liquid	Isopropyl alcohol (≥65%), chlorhexidine bigluconate (≥0.02%).
Shelly™, Ukraine	Universal Disinfectant Spray	Liquid	Propanol, organic solvent, purified water, glycerin, alkyl dimethyl benzyl ammonium chloride, fragrance, vitamin E.
LLC "Petrokos", Ukraine	Antiseptic for Hands	Liquid	Ethyl alcohol, water, lavender extract, glycerin, vitamin E.
MDM GROUP, Ukraine	Hand Antiseptic "Manorm"	Liquid	Isopropyl alcohol 60%, quaternary ammonium compounds 0.11%, excipients: water, glycerin, panthenol, fragrance, dye.
LLC "Ales", Ukraine	Universal Antiseptic "Sani Silver"	Liquid	Alcohol-based compounds 70%, water, glycerin, fragrance composition, aloe extract.
Company "Pharmacom", Ukraine	Antiseptic Hand Lotion	Liquid	Isopropyl alcohol, purified water, glycerin, panthenol.

***Source:** developed by the authors of this study*

As a result of the study, an alcohol-free hand sanitiser was developed, which demonstrated high antimicrobial activity and skin safety. This was an important step towards finding alternatives to widely used alcohol-based antiseptics, which have several significant limitations, such as the ability to cause skin dryness and irritation with frequent use, as well as increased fire hazard (Aodah *et al.*, 2021). The study noted that the use of benzalkonium chloride as the main active ingredient made it possible to create an alcohol-free product that was not only effective in combating microorganisms but also provided a more comfortable experience compared to traditional ethanol gels due to the reduced likelihood of skin irritation. A comparison with other alcohol-free antiseptics developed, for example, by P. Egner *et al*. (2023), showed that the addition of mandelic acid and essential oils (cinnamon, clove, lemon, thyme) to the gels helped to maintain optimal physicochemical characteristics, such as pH and viscosity. At the same time, these additives also improved the antimicrobial activity of the product and ensured the stability of the solution. Similarly, B.-H. Youn *et al.* (2021) demonstrated that essential oils, such as tea tree oil, can also enhance antimicrobial properties and are effective alternatives to alcohol-based antiseptics. This made it possible to create a product that meets the requirements of dermatological safety and ease of use. It was noted that the mixture of essential oils with mandelic acid additionally provided a milder effect on the skin, reducing the risk of allergic reactions with prolonged use.

Given this context, it is important to highlight the issues associated with the use of traditional thickeners, particularly carbomer. S. Sommatis *et al.* (2023) and A. Berardi *et al.* (2020) identified carbomers – also referred to as carboxypolymethylene or Carbopol – as the primary viscosity-enhancing excipients employed in ABHS. These cross-linked polyacrylic acid polymers create a three-dimensional network within their polymer chains, and upon hydration, they expand and uncoil to produce clear, stable, and thick hydroalcoholic formulations with a favorable tactile quality. Nevertheless, M. Marchetti *et al.* (2024) highlighted that the environmental

sustainability of these synthetic polymers is a growing concern, prompting investigation into greener alternatives. Studies by S. Bom *et al.* (2020) and A.M. Martins & J.M. Marto (2023) emphasised issues related to the petrochemical origin of carbomers, their resistance to biodegradation, adverse effects on aquatic ecosystems, and potential residual monomer contaminants. Considering the possible risks associated with the use of carbomer, in order to reduce the likelihood of skin irritation and dryness, moisturising and softening components, in particular propylene glycol, triethylene glycol and cocamidopropyl PG-dimonium chloride phosphate, were included in the development of the product within the framework of this study. The results of organoleptic testing and the determination of physicochemical properties were presented in Table 3.

***Table 3**. Organoleptic and physicochemical characteristics of the tested samples*

Parameter	Sample 1	Sample 2	Sample 3	Sample 4
Appearance	Transparent, homogeneous	Transparent, homogeneous	Transparent, homogeneous	Transparent, homogeneous
pH	4.8 ± 0.2	5.0 ± 0.2	5.2 ± 0.2	5.3 ± 0.2
Viscosity (mPa·s)	22 ± 0.3	23 ± 0.4	24 ± 0.3	23 ± 0.3
Transparency	Transparent	Transparent	Transparent	Transparent
Organoleptic properties	Strong citrus aroma	Mild orange aroma	Lavender aroma, calming	Light woody aroma

***Source:** developed by the authors of this study*

Research by L. Dascalu (Rusu) *et al.* (2020) revealed a strong correlation between the chemical composition of essential oils and their antimicrobial activity. The main active components of lemon, cinnamon, clove and thyme essential oils are limonene, cinnamaldehyde, eugenol and thymol, respectively. They have the ability to disrupt the integrity of microbial cell membranes, leading to the loss of cell contents and cell death. These results are consistent with a study by A. Orchard & S. van Vuuren (2017), which confirmed the antibacterial properties of cinnamaldehyde, the main component of cinnamon oil. Cinnamaldehyde effectively destroys bacterial membranes, making cinnamon oil a promising ingredient for antiseptic agents. Additionally, a study by J. Sedlaříková *et al*. (2019) showed that thymol, the main component of thyme oil, has similar antimicrobial activity by disrupting the membranes of microorganisms. This makes essential oils, particularly thyme oil, important in the fight against bacteria due to their antimicrobial activity and skin safety.

The conducted studies revealed that the addition of *Citrus limon* resulted in a slight decrease in pH to 4.8, while viscosity and transparency remained within the established limits. For Sample 2 (*Citrus sinensis*), the pH was approximately 5.0, with viscosity and transparency remaining within the permissible range. For Sample 3 (*Lavandula angustifolia*), the pH was around 5.2, but an increase in solution viscosity to 24 mPa·s was observed, which may lead to uneven dosing when using a sensor-based dispenser. For Sample 4 (*Melaleuca alternifolia*), the pH was 5.3, and viscosity was 23 mPa·s. All samples were transparent and passed microbiological testing for the absence of pathogenic microorganisms. The quality specification for the finished product of Sample 4 was presented in Table 4. The results indicated that the choice of essential oil significantly affects both the physicochemical properties and the antimicrobial efficacy of the formulations. The inclusion of *Melaleuca alternifolia* provided an optimal balance between pH, viscosity, and transparency, ensuring uniform dosing and compliance with microbiological safety standards. Slight variations in pH observed with other essential oils did not compromise product stability but may influence skin compatibility and sensory perception. The findings highlighted the importance of carefully selecting essential oils not only for their antimicrobial activity but also for their impact on formulation stability, user safety, and application convenience, supporting the development of effective and consumer-friendly alcohol-free hand antiseptics.

***Table 4**. Finished product specification (Sample 4)*

Parameter	Control method	Acceptance criteria	Result	Note
Appearance	Organoleptic	Transparent, homogeneous	Transparent, homogeneous	Complies
pH	pH meter	4.5-6.0	5.3 ± 0.2	Complies
Viscosity (mPa·s)	Rotational viscometer	15-35	23 ± 0.3	Complies
Transparency	Visual inspection	No turbidity	Transparent	Complies
Benzalkonium chloride (%)	Titrimetric, HPLC	0.1-0.15	0.12 ± 0.02	Complies
Microbiological purity	Microbiological analysis	Absence of pathogens	Absence of pathogens	Complies

***Source:** developed by the authors of this study*

The analysis of the results presented in Table 4 demonstrated that the addition of *Melaleuca alternifolia* essential oil provided additional antimicrobial activity and improved the organoleptic properties of the product without affecting solution stability. The developed model alcohol-free hand antiseptic based on benzalkonium chloride meets the

established regulatory requirements for physicochemical and microbiological parameters (World Health Organization, 2009). The transparent and homogeneous appearance confirmed system stability, while a pH of 5.3 ± 0.2 corresponds to the established norm. The solution viscosity of 23 ± 0.3 mPa·s ensures convenient and uniform dispensing using a sensor-based dispenser. Transparency met the regulatory requirements, the concentration of benzalkonium chloride at 0.12% confirmed the accuracy of active ingredient incorporation, and microbiological purity indicated the absence of pathogenic microorganisms. These findings indicated that the incorporation of *Melaleuca alternifolia* not only enhances the antimicrobial efficiency of the formulation but also contributes positively to the sensory characteristics of the product, making it more acceptable for regular use. The pH value within the skin-friendly range suggests minimal risk of irritation, while the observed viscosity ensures precise and reproducible dosing, which is particularly important when using sensor-based dispensers. The compliance with transparency and microbiological standards confirmed the formulation's stability and safety. Overall, the results supported the feasibility of developing alcohol-free hand antiseptics that are both effective against microorganisms and gentle on the skin, aligning with consumer demand for safer, non-alcoholic alternatives.

Conclusions

The conducted studies demonstrated that the developed formulation and technological process for obtaining an alcohol-free antiseptic solution based on benzalkonium chloride and essential oils with antimicrobial properties – involving the preparation of aqueous and antimicrobial phases, their subsequent combination, and incorporation of essential oils – allow the production of a stable and safe product. All four model samples containing different essential oils (*Citrus limon*, *Citrus sinensis*, *Lavandula angustifolia*, and *Melaleuca alternifolia*) met physicochemical and microbiological requirements, exhibiting a transparent and homogeneous structure, skin-friendly pH, and comfortable viscosity. The inclusion of essential oils enabled modulation of organoleptic properties (aroma) without negatively affecting solution stability or antimicrobial efficacy. The pH values ranged from 4.8 for *Citrus limon* to 5.3 for *Melaleuca alternifolia*, remaining within the skin-safe range. Solution viscosities varied between 22 mPa·s (*Citrus limon*) and 24 mPa·s (*Lavandula angustifolia*), ensuring uniform dosing and compatibility with sensor-based dispensers. Transparency measurements confirmed a clear and homogeneous appearance for all samples, while microbiological analysis demonstrated the absence of pathogenic microorganisms, confirming the formulations' safety and antimicrobial efficacy.

The most optimal formulation was the Sample 4 containing *Melaleuca alternifolia*, which combined effective antimicrobial action, pleasant aroma, skin-safe pH (5.3 ± 0.2), and appropriate viscosity (23 ± 0.3 mPa·s) for use with sensor-based dispensers. The benzalkonium chloride concentration of 0.12% in all samples ensured consistent antimicrobial activity while minimising skin irritation, and the addition of humectants and emollients (propylene glycol, triethylene glycol, Cocamidopropyl PG-Dimonium Chloride Phosphate) supported skin hydration and comfort. Further research could focus on expanding the spectrum of tested essential oils, optimising the formulation for enhanced antiviral activity, and conducting long-term stability and sensory studies to evaluate consumer acceptance and practical usability under various environmental conditions. Such studies would contribute to the development of safer, highly effective, and consumer-friendly alcohol-free hand antiseptics suitable for both domestic and professional use.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Abuga, K., & Nyamweya, N. (2021). Alcohol-based hand sanitisers in COVID-19 prevention: A multidimensional perspective. *Pharmacy*, 9(1), article number 64. doi: 10.3390/pharmacy9010064.

[2] Aodah, A.H., Bakr, A.A., Booq, R.Y., Rahman, M.J., Alzahrani, D.A., Alsulami, K.A., Alshaya, H.A., Alsuabeyl, M.S., Alyamani, E.J., & Tawfik, E.A. (2021). Preparation and evaluation of benzalkonium chloride hand sanitizer as a potential alternative for alcohol-based hand gels. *Saudi Pharmaceutical Journal*, 29(8), 807-814. doi: 10.1016/j.jsps.2021.06.002.

[3] Atolani, O., Baker, M.T., Adeyemi, O.S., Olanrewaju, I.R., Hamid, A.A., Ameen, O.M., Oguntoye, S.O., & Usman, L.A. (2020). COVID-19: Critical discussion on the applications and implications of chemicals in sanitizers and disinfectants. *EXCLI Journal*, 19, 785-799. doi: 10.17179/excli2020-1386.

[4] Berardi, A., Perinelli, D.R., Merchant, H.A., Bisharat, L., Basheti, I.A., Bonacucina, G., Cespi, M., & Palmieri, G.F. (2020). Hand sanitisers amid CoViD-19: A critical review of alcohol-based products on the market and formulation approaches to respond to increasing demand. *International Journal of Pharmaceutics*, 584, article number 119431. doi: 10.1016/j.ijpharm.2020.119431.

[5] Bom, S., Ribeiro, H.M., & Marto, J. (2020). Sustainability calculator: A tool to assess sustainability in cosmetic products. *Sustainability*, 12(4), article number 1437. doi: 10.3390/su12041437.

[6] Dalasile, S., Itoba Tombo, E., Madonsela, B.S., Mpungose, P.P., Mshicileli, N., & Menziwa, M. (2024). Alcohol-based hand sanitizers used for COVID-19 prevention in the informal settlements of Cape Town, South Africa. *COVID*, 4(10), 1655-1675. doi: 10.3390/covid4100115.

[7] Dascalu (Rusu), L., Moldovan, M., Prodan, D., Ciotlaus, I., Carpa, R., Ene, R., Sava, S., Chifor, R., & Badea, M. (2020). Antimicrobial activity and chemical composition of two experimental gels based on essential oils. *Studia Universitatis Babeş-Bolyai, Chemistry*, 65(2), 57-67. doi: 10.24193/subbchem.2020.2.05.

[8] Egner, P., Pavlačková, J., Sedlaříková, J., Pleva, P., Mokrejš, P., & Janalíková, M. (2023). Non-alcohol hand sanitiser gels with mandelic acid and essential oils. *International Journal of Molecular Sciences*, 24(4), article number 3855. doi: 10.3390/ijms24043855.

[9] Gupta, D., & More, A. (2021). Alcohol-based hand sanitizer-induced burns: A harsh reality in current times. *Indian Journal of Medical Sciences*, 74(1), 40-43. doi: 10.25259/IJMS_365_2021.

[10] Marchetti, M., Perini, A., Zanella, M., Benetti, F., & Donelli, D. (2024). Study on the fate of the Carbopol® polymer in the use of hand sanitizer gels: An experimental model to monitor its physical state from product manufacturing up to the final hand rinse. *Microplastics*, 3(3), 390-404. doi: 10.3390/microplastics3030024.

[11] Martins, A.M., & Marto, J.M. (2023). A sustainable life cycle for cosmetics: From design and development to post-use phase. *Sustainable Chemistry and Pharmacy*, 35, article number 101178. doi: 10.1016/j.scp.2023.101178.

[12] Ministry of Health of Ukraine. (2025). *State register of disinfectants*. Retrieved from https://data.gov.ua/dataset/reestr_dezzasobiv_moz.

[13] Oder of the Ministry of Health of Ukraine No. 1247 "On Approval of Methodological Recommendations for the Application of Technical Regulations for Cosmetic Products". (2024, June). Retrieved from https://zakon.rada.gov.ua/rada/show/v1247282-24#Text.

[14] Orchard, A., & van Vuuren, S. (2017). Commercial essential oils as potential antimicrobials to treat skin diseases. *Evidence-Based Complementary and Alternative Medicine*, 2017, article number 4517971. doi: 10.1155/2017/4517971.

[15] Perveen, N., Ibrahim, F., & Ansari, A. (2024). Natural hand sanitizers: A systematic review on the effectiveness and antimicrobial potential against pathogens. *Journal of Health & Rehabilitation Research*, 4(3), 1-11. doi: 10.61919/jhrr.v4i3.1131.

[16] Pokryshko, O.V., & Pyatkovskyy, T.I. (2025). Alcohol based hand sanitizers in Ukraine: A comparative evaluation of their effectiveness. *Perspectives and Innovations in Science*, 6(52), 1683-1696. doi: 10.52058/2786-4952-2025-6(52)-1683-1696.

[17] Rafizadeh, A., Kolahi, A.A., Shariati, S., Zamani, N., Roberts, D.M., & Hassanian-Moghaddam, H. (2023). The danger of the toxicity and inefficacy of alcohol-based hand rubs in Iran during COVID-19: A cross-sectional study. *Antimicrobial Resistance & Infection Control*, 12, article number 42. doi: 10.1186/s13756-023-01244-w.

[18] Resolution of the Cabinet of Ministers of Ukraine No. 753 "On the Approval of the Technical Regulation on Medical Devices". (2013, October). Retrieved from https://zakon.rada.gov.ua/laws/show/753-2013-%D0%BF#Text.

[19] Resolution of the Cabinet of Ministers of Ukraine No. 863 "On Approval of the Regulations on State Registration of Disinfectants". (2023, August). Retrieved from https://www.kmu.gov.ua/npas/pro-zatverdzhennia-polozhennia-pro-derzhavnu-reiestratsiiu-dezinfektsiinykh-zasobiv-863-150823.

[20] Saha, T., Khadka, P., & Das, S.C. (2021). Alcohol based hand sanitizer – composition, proper use and precautions. *Germs*, 11(3), 408-417. doi: 10.18683/germs.2021.1278.

[21] Sedlaříková, J., Janalíková, M., Rudolf, O., Pavlačková, J., Egner, P., Peer, P., Varaďová, V., & Krejčí, J. (2019). Chitosan/thyme oil systems as affected by stabilizing agent: Physical and antimicrobial properties. *Coatings*, 9(3), article number 165. doi: 10.3390/coatings9030165.

[22] Sommatis, S., Capillo, M.C., Maccario, C., Rauso, R., D'Este, E., Herrera, M., Castiglioni, M., Mocchi, R., & Zerbinati, N. (2023). Antimicrobial efficacy assessment and rheological investigation of two different hand sanitizers compared with the standard reference WHO formulation 1. *Gels*, 9(2), article number 108. doi: 10.3390/gels9020108.

[23] Večerková, L., Mašková, L., Knejzlík, Z., Kašpar, O., & Tokárová, V. (2024). Development of spray dried powder hand sanitiser with prolonged effectivity. *Scientific Reports*, 14, article number 4827. doi: 10.1038/s41598-024-55503-w.

[24] Villa, C., & Russo, E. (2021). Hydrogels in hand sanitizers. *Materials*, 14(7), article number 1577. doi: 10.3390/ma14071577.

[25] World Health Organization. (2009). *Guidelines on hand hygiene in health care: First global patient safety challenge. Clean care is safer care.* Retrieved from https://www.who.int/publications/i/item/9789241597906.

[26] Youn, B.-H., Kim, Y.-S., Yoo, S., & Hur, M.H. (2021). Antimicrobial and hand hygiene effects of tea tree essential oil disinfectant: A randomised control trial. *International Journal of Clinical Practice*, 75(8), article number e14206. doi: 10.1111/ijcp.14206.

Розробка складу та технології безспиртового антисептичного засобу для рук

Ганна Тарасенко
Кандидат технічних наук, доцент
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
https://orcid.org/0000-0002-0995-7322
Олена Салій
Кандидат фармацевтичних наук, доцент
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
https://orcid.org/0000-0001-7103-2083
Богдан Муравский
Магістр
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
https://orcid.org/0009-0009-6511-8222
Марія Попова
Аспірант
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
https://orcid.org/0000-0002-2579-0331
Галина Кузьміна
Кандидат хімічних наук, доцент
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
https://orcid.org/0000-0002-0691-8563

Анотація. Ефективна гігієна рук є ключовою умовою профілактики інфекційних захворювань, що зумовлює потребу у безпечних та високоефективних антисептичних засобах і підкреслює актуальність розробки формул з оптимальними антимікробними, дерматологічними та технологічними властивостями. Метою дослідження була розробка безспиртового антисептичного засобу для рук із високою антимікробною активністю, безпечністю для шкіри та можливістю застосування сумісністю з сенсорними дозаторами. Аналіз ринку антисептичних засобів здійснювали з використанням аналітично-статистичних методів, а визначення показників якості антисептичного засобу проводили із застосуванням органолептичних, фізико-хімічних та мікробіологічних методів контролю. Встановлено, що на ринку антисептичних засобів домінують препарати на основі етилового, пропілового та ізопропілового (понад 70 %), а також визначено їхні основні обмеження, зокрема здатність викликати сухість шкіри та ризик подразнення при постійному застосуванні, а також їх підвищену пожежонебезпечність. На основі проведеного аналізу запропоновано безспиртову композицію, у якій бензалконію хлорид (0,1-0,15 %) визначено оптимальним активним компонентом. Досліджено чотири варіанти складу з різними ефірними оліями; встановлено, що зразки мали pH у межах 4,8-5,3 та в'язкість 22-24 мПа•с. Зразок з *Melaleuca alternifolia* продемонстрував найкраще співвідношення показників – pH 5,3 ± 0,2, в'язкість 23 ± 0,3 мПа•с, прозорість та стабільність, а також покращені органолептичні властивості. Усі зразки відповідали мікробіологічним вимогам, а вміст бензалконію хлориду становив 0,12 ± 0,02 %, що підтверджує точність дозування. Запропоновано технологічний процес одержання засобу шляхом приготування двох фаз із подальшим їх об'єднанням, що забезпечило стабільність та однорідність готового продукту. Результати роботи можуть бути використані виробниками косметичних і дезінфекційних засобів для створення безспиртових антисептиків, придатних до застосування у медичних, освітніх, соціальних установах та побутових умовах, зокрема в приладах для антисептичної обробки рук з сенсорними дозаторами

Ключові слова: гігієнічний засіб; бензалконію хлорид; ефірна олія; розчинення; гігієнічна обробка рук; сенсорний дозатор

ТЕХНОЛОГІЇ ТА ІНЖИНІРИНГ

Науковий журнал

Том 26, № 4, 2025

Оригінал-макет видання виготовлено
у редакційно-видавничому відділі Київського національного університету технологій та дизайну

Відповідальний редактор:
О. Кривонос

Підписано до друку 17.09.2025 р. Формат 60*84/8
Умовн. друк. арк. 9,1
Наклад 100 примірників

Адреса видавництва:
Київський національний університет технологій та дизайну
01011, вул. Мала Шияновська, 2, м. Київ, Україна
тел/факс: +38 (044) 256-84-27
E-mail: knutd@technologies-engineering.com.ua
https://technologies-engineering.com.ua/uk

TECHNOLOGIES AND ENGINEERING

Scientific Journal

Vol. 26, No. 4, 2025

The original layout of the publication is made
in the publishing department of Kyiv National University of Technologies and Design

Managing editor:
O. Kryvonos

Signed for print 17.09.2025. Format 60*84/8
Conventional printed pages 9.1
Circulation 100 copies

Publishing Address:
Kyiv National University of Technologies and Design
01011, 2 Mala Shyianovska Str., Kyiv, Ukraine
tel/fax: +38 (044) 256-84-27
E-mail: knutd@technologies-engineering.com.ua
https://technologies-engineering.com.ua/en