Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 22, No. 3. 2025**

Article's History: Received: 15.08.2025 Revised: 11.11.2025 Accepted: 23.12.2025

UDC 004.056.5:004.032.26 DOI: 10.31649/vitce/3.2025.148

Synergy of artificial intelligence, SDN, Zero Trust, and blockchain: An overview of new trends in secure network management

Oleksandr Pidpalyi*

PhD
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0009-0007-6852-7959

Oleksandr Romanov

Doctor of Technical Sciences, Lecturer
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-8683-3286

Abstract. The research relevance is determined by the need to create effective, transparent, and cyberattack-protected network management systems. The study aimed to systematise and critically analyse current approaches to combining artificial intelligence, software-defined networks, Zero-Trust architecture and blockchain to build adaptive, transparent and cyberattack-proof network management systems. A conceptual review of secure network management technologies was conducted using interpretative and comparative analysis of scientific sources, systemic and structural-categorical analysis of the characteristics of software-defined networks, Zero Trust architecture, blockchain, and artificial intelligence, and modelling scenarios for their application to improve the adaptability, transparency, and resilience of network systems in critical sectors of Ukraine. The results showed that the combined use of these technologies provides centralised traffic management, dynamic access policies, transparency of operations, and the ability to autonomously detect threats, significantly increasing the resilience of the network to multi-vector cyber-attacks. The study determined that the main problems of integrating these technologies into network systems are the opacity of artificial intelligence solutions, conflicts between the dynamism of models and the immutability of blockchain, high resource requirements, and the complexity of policy coordination in multi-domain networks. The implementation of Explainable Artificial Intelligence, hybrid architectures, off-chain solutions, model optimisation, and federated protocols has overcome limitations, providing a transparent, adaptive, and secure network system capable of responding effectively to threats and dynamic changes in the environment. The results showed that traditional solutions based on static firewalls and centralised control are limited in terms of response speed, attack detection accuracy and scalability. Integrated models combining artificial intelligence, software-defined networking, Zero-Trust architecture, and blockchain provide instant threat response, highly accurate attack detection, dynamic access control, automated auditing, and effective scalability, creating an adaptive, resilient, and transparent network system. The results of the study can be used to develop and optimise cybersecurity policies, automate access control and network event monitoring, and build scalable and transparent architectures of management systems

Keywords: network security; cyber defence; intrusion detection; machine learning; explainable artificial intelligence

Introduction

The growing complexity of cyber threats renders traditional network security models based on static policies and perimeter protection ineffective. Modern attacks bypass classic defence mechanisms, creating a need for dynamic solutions capable of detecting anomalies in real time and adaptively changing access policies. The combination of artificial intelligence (AI), Software-Defined Networking (SDN), Zero Trust Architecture (ZTA) and blockchain

Suggested Citation:
Pidpalyi, O., & Romanov, O. (2025). Synergy of artificial intelligence, SDN, Zero Trust, and blockchain: An overview of new trends in secure network management. *Information Technologies and Computer Engineering*, 22(3), 148-163. doi: 10.31649/vitce/3.2025.148

*Corresponding author

creates the basis for new approaches to security management. AI provides traffic and user behaviour analysis, SDN provides a flexible infrastructure, ZTA enables micro-segmentation and dynamic authentication, and blockchain ensures the immutability of event logs. For Ukraine, such synergy is necessary in the context of protecting critical infrastructure and government electronic services from hybrid threats.

The issue of integrating technologies to improve the adaptability and security of network systems was addressed by Ukrainian scientists. V.S. Nikitchenko (2024) studied the trends of digital transformation of business structures in the context of Industries 4.0 and 5.0, paying attention to the integration of modern technologies to improve the adaptability and efficiency of enterprises. The study demonstrated that the comprehensive implementation of automated control systems and decentralised technologies, such as blockchain and AI, can significantly increase the reliability of business processes, which directly correlates with approaches to the integration of SDN, ZTA and blockchain in secure network environments. These findings confirm the relevance of combining several technologies to ensure the adaptability and transparency of network systems. In turn, M.V. Vorokhob (2023) analysed models and methods for the improvement of enterprise security policies based on the Zero Trust methodology. The study emphasised that the implementation of behavioural access control models, continuous user monitoring and dynamic policy adaptation is key to reducing the risks of insider threats and ensuring the reliability of multi-domain networks. These concepts correlate with the use of AI+ZTA in practical scenarios of integrated network management, where AI behavioural algorithms assess user risk and automatically adapt access rights.

S.A. Latif *et al*. (2022) proposed a comprehensive security architecture for IoT networks of cyber-physical systems, integrating AI, blockchain, and SDN. The study demonstrated that this combination not only automates anomaly detection and attack prediction but also ensures real-time data transparency and immutability. These results confirm the feasibility of using multi-component solutions to improve the resilience of critical network infrastructures. At the same time, M.H. Bashaa *et al.* (2025) reviewed the integration of ZTA and machine learning (ML) to improve the security of software-defined networks. The study determined that the combined use of behavioural models, adaptive access policies, and AI for threat prediction significantly improves attack detection accuracy and enables rapid response to incidents. The authors also emphasise the relevance of audit and monitoring automation, which is consistent with practical cases of integrated network solutions implementation in various industries. L. Alevizos *et al.* (2022) considered the issue of extending ZTA to endpoints using blockchain. The study determined that the integration of decentralised registries increases the system's resistance to attacks and ensures audit transparency. The study emphasised that combining ZTA and blockchain helps protect critical network components and boosts trust in secure access management in corporate environments. This approach is relevant to the analysis of the potential of integrated network security solutions that combine ZTA and decentralised technologies.

S. Tiwari *et al.* (2022) proposed an approach to integrating AI with ZTA to improve the adaptability of network security in modern cyber threats. The study showed that AI can be used for real-time assessment of user and device behaviour and automatic adjustment of access policies, which significantly reduces the risk of security breaches. The study emphasised the potential of combining AI and ZTA to increase the flexibility and effectiveness of multi-domain network protection. B. Chowdhury *et al.* (2023) presented a conceptual model of a digital twin for e-Healthcare based on 6G using Zero Trust and blockchain. AI-driven attack prediction and response mechanisms, combined with decentralised registries, have been shown to enhance the security of critical healthcare systems. This approach demonstrates the practical benefits of integrated solutions in the context of protecting confidential data and ensuring service continuity. At the same time, A.V. Nagarjun & S. Rajkumar (2024) conducted a comprehensive review of the potential of deep learning and blockchain for intrusion detection systems (IDS). The study determined that the combination of AI and blockchain increases the accuracy and speed of anomaly detection while ensuring the transparency and immutability of event logs. This approach supports the idea of creating adaptive, autonomous security systems that can effectively respond to complex and multi-vector threats.

An analysis of previous studies demonstrated that existing studies are mostly limited to theoretical models or the analysis of individual corporate cases, without covering their interaction in scalable environments focused on the public sector and critical infrastructure. This creates a gap in the scientific and applied justification of integrated solutions that combine AI, SDN, Software-Defined Wide Area Network (SD-WAN), ZTA, and blockchain into a robust network management system. The study aimed to systematise and critically analyse current research on the integration of AI, SDN, ZTA and blockchain technologies to create adaptive, transparent and cyber-resilient network management systems. To achieve this goal, the following tasks were set: to identify and analyse existing approaches and models for integrating these technologies into network systems, to evaluate their effectiveness and limitations; to identify synergies between components, key challenges and prospects for the further development of integrated adaptive network solutions.

Materials and Methods

A conceptual review of modern technologies for secure network management and their integration was conducted to improve the adaptability, transparency, and resilience of telecommunications systems to multi-vector cyber threats. From the overall pool of scientific and scholarly

publications published between 2021 and 2025, a total of 34 academic sources met the inclusion criteria and were thematically relevant to the scope of the study. However, only a subset of these sources was directly employed in the formulation of comparative results and in the modelling of integrated network scenarios (AI + SDN + ZTA + blockchain). The remaining sources primarily served a supportive role, contributing to the development of the conceptual framework, the theoretical grounding of the study, and the enrichment of the discussion concerning limitations, risks, and future directions of technology integration. The literature search was conducted using major international scientific databases, including Scopus, Web of Science Core Collection, IEEE Xplore, ACM Digital Library, and ScienceDirect, which ensured comprehensive coverage of peer-reviewed research in the fields of network engineering, cybersecurity, and information systems.

Criteria for inclusion of sources works describing the integration of these technologies into network systems, research on Zero Trust architectural solutions, the use of AI for threat prediction or security policy automation, as well as reviews and comparative studies of security models. Criteria for excluding sources: publications that do not contain specific data on the integration of technologies or their impact on the adaptability and resilience of networks, works that deal exclusively with hardware solutions without elements of SDN, ZTA, blockchain or AI, and materials published before 2021. The research was conducted from March to August 2025.

The research methodology involved systematising and conducting a comparative analysis of the characteristics of each technology. The method of interpretative analysis of scientific sources was used to evaluate the architecture, tasks and functional capabilities of AI, SDN, ZTA and blockchain, as well as the method of comparative analysis to compare their advantages and limitations in the context of building integrated network solutions. To structure the data obtained, a method of systematic and structural-categorical analysis was used, which facilitated the organisation of technology characteristics into logical blocks and the creation of analytical tables. This facilitated a detailed description of the key functions of the technologies, their application scenarios, advantages for security and network management, potential limitations and ways to overcome them, as well as a comparison of traditional and integrated security models.

Modelling of integrated scenarios for the application of technologies in networks was highlighted. To assess the advantages of integrated solutions, an analysis of technical and organisational aspects was conducted, including increased network adaptability and flexibility, automated threat detection and access control, ensuring data transparency and immutability, as well as scalability and integration into multi-domain networks. Potential challenges and limitations of technology integration were also explored, including explainable AI issues, conflicts between AI and blockchain dynamics, high computing resource requirements and policy coordination in multi-domain networks, as well as ways to overcome them. A comparative analysis of traditional network security models and integrated solutions (AI + SDN + ZTA + blockchain) was conducted based on the criteria of incident response speed, attack detection accuracy, scalability, resistance to internal threats, transparency and auditability, adaptability to dynamic changes, and level of automation.

The study examined application-orientated conceptual scenarios for deploying integrated AI, SDN, ZTA, and blockchain in Ukraine. These scenarios were not treated as fully documented, organisation-specific case studies with proprietary network datasets; rather, they represent desk-based modelling and feasibility assessment grounded in (i) the reviewed scientific literature on AI/SDN/ZTA/blockchain integration and (ii) open policy and industry documents that describe reference architectures, maturity targets, and automation principles for multi-domain networks. Three scenario classes were analysed. First, public e-service delivery environments (including high-assurance digital service platforms) were modelled as ZTA-enabled service perimeters in which AI supports anomaly detection and risk-based access decisions, while a permissioned ledger provides tamper-evident audit trails for security-relevant events. Second, critical infrastructure communications and control-support networks were analysed at the level of architectural patterns: SDN enables rapid traffic engineering and segmentation, AI performs predictive detection of abnormal behaviour, and ledger-based logging strengthens traceability and accountability of configuration and access actions. Third, multi-domain government networks were considered as simulated, federated environments within a conceptual modelling framework, in which ZTA enforces continuous verification, AI automates behavioural monitoring, and blockchain-backed audit logs enhance cross-domain accountability. Consequently, the information basis for these scenarios was derived primarily from analysed reports, standards, and industry architecture documents, while the academic corpus was used to substantiate technical feasibility, integration constraints, and expected effects. These cases are therefore reported as simulation-based conceptual implementations rather than empirical evaluations of named Ukrainian networks or operational systems.

The study also developed recommendations for the development of a national AI ecosystem, standardisation and integration of technologies, staff training and cooperation with international partners to implement integrated solutions in critical infrastructures. In addition, industry reports and documents regulating the implementation of integrated network solutions and approaches were analysed. The Memorandum for the Heads of Executive Departments and Agencies (2022), DoD Zero Trust Strategy (2022), AT&T Domain 2.0 Vision White Paper (2013), and Telefónica (2017) approaches were reviewed. In addition, LF Networking projects focused on the Open Network Automation Platform (Alhilali & Montazerolghaem, 2023) were analysed. The analysis of these cases revealed real

models of AI, SDN, ZTA, and blockchain integration, security policy standardisation, automation and audit principles in multi-domain networks, and key practical approaches to improving the cyber resilience and adaptability of network systems. Visualisation and modelling of data flows in the network were conducted using block diagrams illustrating the sequence of traffic processing, cyclical interaction of components, feedback mechanisms, and real-time self-regulation of the system. This was to assess not only the functional capabilities of individual technologies, but also their synergy in ensuring adaptive and autonomous network management.

Results and Discussion

Overview of basic technologies for secure network management

The review demonstrated how key components such as SDN, ZTA, blockchain, and AI interact to enable adaptive and secure network management. These technologies complement each other, providing centralised management, dynamic access policies, operational transparency, and autonomous threat detection capabilities. SDN represents an architecture with a separation of control plane and data plane; the SDN controller centrally manages traffic flows and sets routing policies on switching devices. AI integration can detect traffic anomalies, predict possible attacks, and dynamically redirect flows based on network conditions. SDN also provides event logging and real-time monitoring of network resources. ZTA implements the "zero trust" principle: the network is segmented into isolated zones (microsegmentation), and each user and device undergoes adaptive authorisation with constant verification. Access control is based on behavioural models and risk-oriented algorithms, which can be used to change access rights quickly depending on the threat (Aramide, 2024). For a systematic comparison of key secure network management technologies, their main characteristics, functions and integration capabilities are summarised in Table 1.

Table 1. Key features of technologies for secure network management

Technology	Key functions	Integration with other components	Main benefits	Potential limitations
SDN	Centralised traffic management, dynamic routing	AI for anomaly prediction and policy optimisation	Adaptability, quick response	Dependence on the controller, high resource requirements
ZTA	Adaptive access control, micro-segmentation	AI for behavioural assessment of users	Reduction of internal threats, dynamic authorisation	Complexity of implementation, need for constant verification
Blockchain	Decentralised storage, smart contracts	AI for log verification and auditing	Transparency, data consistency	Conflict with AI dynamics, transaction delays
AI (ML/DL/RL)	Traffic classification, anomaly detection	SDN for routing, ZTA for access, blockchain for logs	Automation, adaptability, threat prediction	Explainability (XAI), need for computational resources

Note: DL – deep learning; RL – reinforcement learning
Source: compiled by the authors based on analysis of data of H. Han *et al*. (2021), P. Svensberg (2023), A. Alshehri *et al*. (2024), F. Ashfaq *et al.* (2025)

Analysis of Table 1 shows that each considered technology is specific but complementary in secure network management. SDN provides centralised traffic management and provides a rapid response to changes in the network, but its dependence on a controller and high computing resource requirements are potential limitations. ZTA effectively reduces the risks of internal threats through adaptive access control and micro-segmentation, but it requires constant user verification and complex policy configuration. Blockchain increases data transparency and immutability and provides automated auditing, but the dynamic nature of AI models can conflict with transaction delays and the need for consensus in the network. AI in network solutions provides threat prediction, traffic classification, and adaptive security policy management, but requires explainability of decisions and significant computing resources.

The interconnection of these technologies compensates for the limitations of individual components: SDN integration with AI provides dynamic routing and anomaly detection; the combination of AI and ZTA ensures adaptive access control; blockchain supports transparency and immutability of actions. Thus, the combined use of SDN, ZTA, blockchain, and AI forms a comprehensive system that simultaneously increases the security, adaptability, and reliability of the network infrastructure. O. Aramide (2022) examines the principles of Zero Trust identity with continuous AI verification in next-generation networks. The study specifies that AI integration enables the creation of secure digital ecosystems with adaptive access control based on behavioural identities. This directly correlates with the ability to create secure digital ecosystems with adaptive access control based on behavioural identities. The study specifies that AI integration can be used to create secure digital ecosystems with adaptive access control based on behavioural identities. This directly correlates with the current approach to integrating XAI models into access policies: the study also emphasises the role of explainability and continuous verification. At the same time, O. Aramide focuses primarily on the user identity level, while the current study pays considerable attention to the network plane (SDN, policy-as-code). Figure 1 shows an integrated network architecture that combines SDN, the ZTA concept, and blockchain technologies.

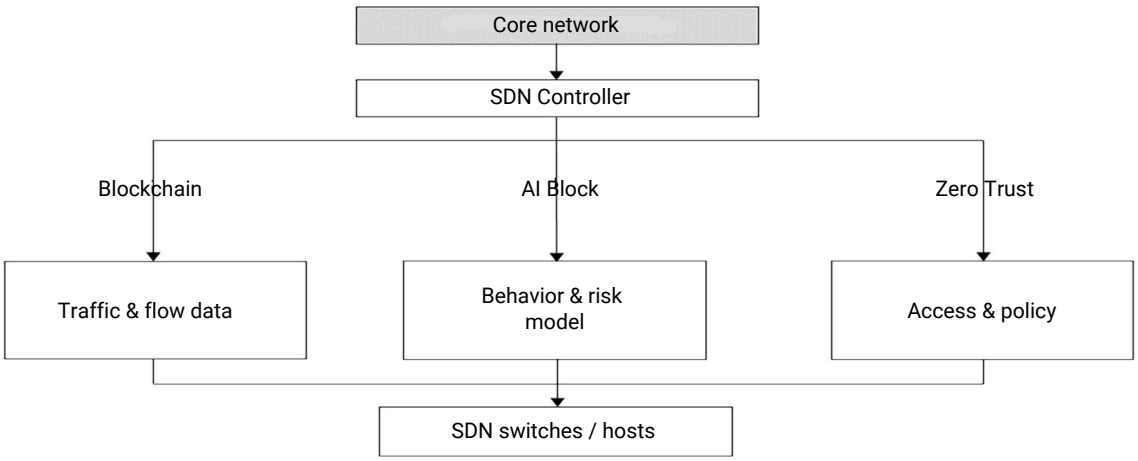

Figure 1. AI block integration diagram
Source: compiled by the authors based on analysis of F. Ashfaq *et al.* (2025)

The AI block is located between the SDN controller and the Zero Trust and blockchain system components. It performs adaptive analysis of traffic and user behaviour, which can be used for dynamic changes to routing and access policies. Log and transaction data are stored in blockchain, and AI analyses it for anomalies and threats. Interaction with the Zero Trust module ensures continuous verification of users and devices, while SDN provides flexible flow management. This integration creates a closed loop of adaptive network management with a high level of transparency, automation, and resistance to cyberattacks. To illustrate the interaction of key technologies in secure network management, a diagram is provided that shows the data flows and roles of each component (Fig. 2).

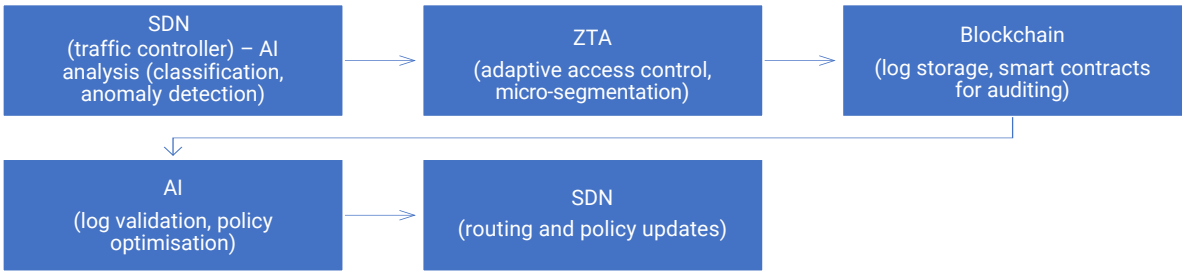

Figure 2. Integration scheme for technologies in a secure network
Source: compiled by the authors based on analysis of P. Svensberg (2023)

An analysis of the SDN, ZTA, blockchain, and AI integration scheme demonstrates a clear sequence of component interactions and the synergistic operation of all elements of the secure network management system. The SDN controller centrally manages traffic flows and provides primary data routing, while the received packets are sent for processing by AI models for traffic classification, anomaly detection, and potential threat prediction. Based on the AI results, the ZTA system adaptively adjusts user and device access rights using micro-segmentation and dynamic authorisation policies. All transactions and actions are recorded in the blockchain, which ensures data immutability, transparency, and the ability to perform automated audits through smart contracts. AI also interacts with blockchain to verify logs, evaluate policy correctness, and correct SDN routing in real time. This cyclical process creates a dynamic, adaptive, and attack-resistant network system where each technology compensates for the limitations of the others. SDN provides centralised management, ZTA enhances access security, blockchain ensures data transparency and immutability, and AI coordinates adaptability and threat prediction. As a result, the integrated system can respond to multi-vector cyberattacks, dynamically change routes and access policies, and maintain a high level of trust in network interactions.

Conceptual overview of scenarios for the application of integrated network technologies

Modern telecommunications systems face the need to ensure high adaptability and resistance to multi-vector attacks. The integration of AI, SDN, ZTA, and blockchain technologies creates new opportunities for automating network management, dynamic access control, and ensuring transparency of operations. To systematise these approaches, basic application scenarios were developed to assess the role of each technology and the effectiveness of their synergy in various aspects of security and network management (Table 2).

Table 2. Conceptual overview of scenarios, technologies, functions and advantages of using integrated network technologies

Use scenario	Employed technologies	Primary functions	Security and network management benefits
Dynamic routing	AI + SDN	ML models analyse traffic and adjust routing rules via an SDN controller	Optimisation of data flows, rapid response to anomalies, and increased network bandwidth
Adaptive access control	AI + ZTA	Behavioural models assess user and device risk, dynamically changing access rights	Reduction of internal risks, micro-segmentation, and increased trust in access
Audit and logging	AI + blockchain	Logging of all actions in a decentralised registry, analysis of logs for anomalies	Data integrity, transparency of operations, and rapid detection of incidents
Comprehensive scenario	AI + SDN + ZTA + blockchain	Integration of all components: threat detection, access policy adaptation, logging	Autonomy, resistance to multi-vector attacks, real-time adaptability, transparency and auditing

Source: compiled by the authors based on O. Aramide (2022) and S. Narayanan (2025)

The table shows four key scenarios for technology integration. In the dynamic routing scenario, ML models act as the analytical core, evaluating network flows and determining optimal routes. SDN is central in quick application of these decisions to network controllers, reducing latency and avoiding congestion. The adaptive access control scenario shows how AI and ZTA collaborate to evaluate user and device behaviour patterns, identifying risks in real time. This enables dynamic access rights management and micro-segmentation, which is critical for protecting internal network segments from potential threats. The audit and logging scenario demonstrates the advantages of blockchain combined with AI: immutable records and smart contracts ensure transaction transparency, while AI analyses logs to quickly detect anomalies and potential incidents. A comprehensive integration scenario for all technologies ensures maximum synergy: SDN centrally manages traffic flows, AI predicts threats and optimises policies, ZTA adaptively controls user access, and blockchain provides reliable auditing and immutability of logs. This approach creates an autonomous, resilient, and transparent network system capable of responding to changes in user behaviour, network load, and new types of threats in real time. A general analysis of the table shows that each technology performs a specific but interrelated function, and their synergy improves security and network management efficiency compared to traditional static solutions. The complexity of implementing such scenarios requires careful balancing of resources, policy coordination, and explainable AI to increase trust in decisions (Chaudhry, 2025). At the same time, S. Batewela *et al.* (2025) examined the challenges of security orchestration in next-generation networks. They conducted a comprehensive review of existing approaches and emphasised the need for integrated solutions capable of coordinating security policies across different network domains. This correlates with the current SDN-based "policy-as-code" approach and closed loops with AI; the contribution of the conducted research is to add immutable auditing and cross-agency interoperability through federated protocols. While scientists address operators and SOAR/IBN chains, the presented analysis details how to combine these chains with blockchain without losing response time (off-chain + periodic commit to the registry).

To illustrate the interaction of technologies in network systems, a block diagram was created that shows data flows, the roles of each component, and cyclical interaction in real time (Fig. 3). The diagram illustrates how AI analyses traffic and predicts threats, SDN provides centralised route management, ZTA implements dynamic access control, and blockchain ensures transparency and immutability of logs. It can be used to evaluate both the sequence of data processing and parallel flows, emphasising the complexity of integrated solutions.

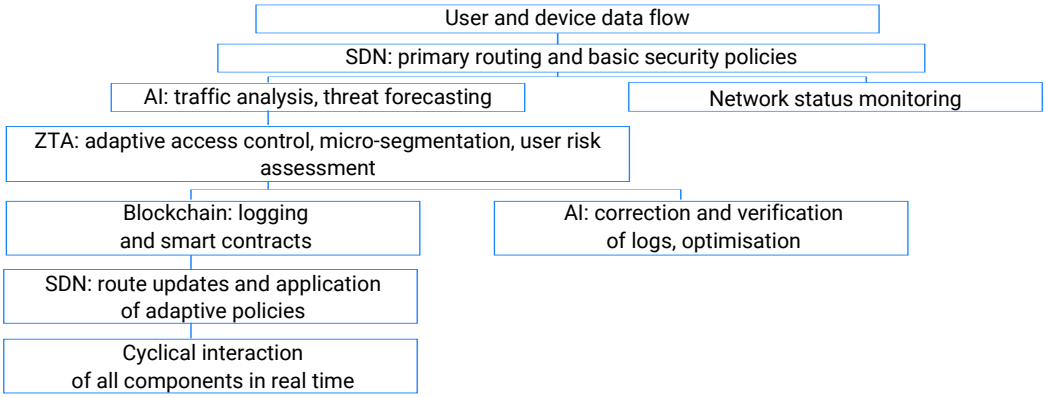

Figure 3. Interaction of technologies in network systems

Source: compiled by the authors based on S. Batewela *et al.* (2025)

The figure shows the step-by-step processing of network flows and the interaction of technologies. At the first level, user and device data are sent to SDN, which performs initial routing and applies basic security policies. At the same time, network status monitoring and traffic analysis are performed through AI modules, which can detect anomalies and predict potential threats. At the second level, ZTA implements adaptive access control, assessing user and device risks in real time, while blockchain records all events in a decentralised registry, ensuring the immutability and transparency of records. AI is used to verify blockchain logs and correct access and routing policies, creating a feedback and self-regulating mechanism for the system. At the third level, SDN applies adaptive routing policies, and redirects flows, and the interaction cycle is repeated in real time, ensuring constant adaptation of the system to changes in user behaviour, network topology and potential threats. Analysis of the diagram shows that each technology performs a specific but interrelated function: SDN is responsible for operational flow management, AI for analysis and forecasting, ZTA for adaptive access control, and blockchain for auditing and transparency. This architecture ensures system autonomy, high adaptability to changes in the network environment, and comprehensive protection against multi-vector attacks, while emphasising the need for policy coordination and optimisation of computing resources.

Analysis of the advantages of integrated solutions in network security

Integrated network security solutions enable a comprehensive approach to protecting digital infrastructures by combining different technologies into a single flexible system. This approach not only provides resilience against the growing number of cyber threats but also improves resource management efficiency and network scalability. First, integrated systems significantly increase network adaptability and flexibility by enabling rapid response to new threats, real-time changes to access and protection policies, and adaptation to different environments. This is a priority for dynamic infrastructures such as cloud services or corporate multi-domain networks. The second advantage is the automation of threat detection and access management, which minimises the human factor and reduces response time. The use of AI and ML can quickly identify traffic anomalies, block malicious actions, and promptly update security rules. Transparency and immutability of data are crucial, which is achieved using blockchain and distributed ledger technologies. This ensures trust in audit results, prevents unauthorised interference, and creates conditions for the formation of a unified information picture across the entire organisation. Lastly, integrated solutions provide scalability and integration into multi-domain networks where different technologies and protocols are used simultaneously. Thanks to their modularity and flexible architectural approaches, such systems can be easily expanded without losing performance and functionality. This creates the basis for the sustainable development of digital infrastructures in the future. For clarity, the main advantages of integrated solutions in network security are presented in Table 3.

Table 3. Advantages of integrated network security solutions

Area of expertise	Key aspects	Importance of network security
Improving network adaptability and flexibility	Dynamic routing, load balancing, integration with SDN	Ensures rapid response to traffic changes, reduces the risk of overload and downtime
Automated threat detection and access control	Using AI/ML for IDS/IPS, Zero Trust, and automated access policies	Minimises human error, accelerates attack neutralisation, and guarantees access control at all levels
Ensuring transparency and consistency of data	Real-time logging and monitoring, blockchain technologies, and SIEM platforms	Increases trust in the system, prevents unauthorised changes, and ensures the verifiability of events
Scalability and integration into multi-domain networks	Cloud and hybrid environments, modular architectures, API integrations	Ensures flexible infrastructure expansion and simplifies management of complex distributed networks

Source: compiled by the authors based on R. Dwivedi *et al*. (2023), A. Malik *et al*. (2025)

The table shows that the advantages of integrated solutions cover both technical and organisational aspects of security. The combination of adaptability and flexibility can ensure network resilience even in rapidly changing cyber threat environments. Automation significantly reduces response time to attacks and reduces dependence on the human factor. Transparency and data immutability increase the level of trust in the system from both users and regulators, which is a priority in the context of regulatory compliance. Lastly, scalability and multi-domain integration make the system flexible from a strategic perspective, which can be used for quick expansion without significant investment in infrastructure restructuring. Thus, integrated network security solutions are not only a technological tool, but also a strategic approach to building secure and flexible digital environments.

Assessment of challenges and limitations of network technology integration

The integration of AI, SDN, ZTA, and blockchain technologies comes with a bunch of challenges, both technical and organisational. One key thing is XAI, as modern ML and DL models often work like “black boxes”, which restricts the ability of administrators and analysts to determine the logic behind the decisions. The opacity of AI algorithms complicates auditing, control, and user trust, which can

potentially lead to incorrect or untimely responses to threats. The use of XAI, standardised documentation of decisions and visualisation of model logic ensures transparency, controllability and soundness of decision-making, which in turn contributes to increased integration efficiency and trust in the system on the part of users and administrators. There is a significant conflict between the dynamism of AI and the immutability principle of blockchain technologies. AI models require constant updating for adaptive network policy management and rapid response to threats, while blockchain ensures the immutability of records and transactions. This creates a potential contradiction that can hinder the synchronisation and coordination of network processes. To overcome this, hybrid architectures, off-chain update mechanisms, and conditionally adaptive smart contracts are used to maintain AI adaptability while ensuring the immutability of data and logs (Speith, 2022).

Another substantial limitation is the high resource intensity of integrated solutions, which arises from the simultaneous use of complex AI models and decentralised blockchain registries. Increased load on computing resources can reduce system performance, increase data processing delays, and limit network scalability. To optimise these processes, lightweight model architectures, pruning and quantisation, as well as distributed computing and cloud computing platforms, are used. This approach ensures effective network adaptability while maintaining response speed and threat prediction accuracy. In addition, the coordination of security policies in multi-domain networks remains critical, as different domains or organisations may use different access, control, and authentication standards. The lack of uniform protocols can lead to conflicts, duplication of rules, and reduced effectiveness of integrated solutions. The use of federated protocols, unified standards, and integration mechanisms can coordinate policies across domains, maintain centralised control, and preserve the autonomy of individual network segments (Pemmasani *et al.*, 2025). This provides a balance between flexibility, security, and compatibility of heterogeneous network environments. Below is a summary Table 4, which systematises the key challenges and possible ways to overcome them.

Table 4. Challenges, problems, limitations and ways to overcome them

Challenge/limitation	Issue	Potential solutions
XAI	AI algorithms are often "black boxes"; it is difficult to explain their decisions	Implementation of XAI, decision documentation standards, and model visualisation
Conflicts between the dynamism of AI and blockchain	AI requires model updates, and blockchain ensures immutability	Hybrid architectures, off-chain solutions, conditionally adaptive smart contracts
High demands on computing resources	AI+blockchain requires significant resources	Cloud services, distributed computing, model optimisation
Policy coordination in multi-domain networks	Different domains have unique security standards	Federated protocols, integration standards, unified access rules

Source: compiled by the authors based on Z. Azam *et al.* (2023)

Following the table, these challenges are closely interrelated: the transparency of AI decisions affects integration with blockchain, resource constraints determine the need for optimisation, and the use of distributed computing and multi-domain conflicts requires the unification of standards and protocols. The comprehensive use of the proposed solutions creates an adaptive, transparent, and secure network system capable of effectively responding to modern threats and dynamically changing operating conditions.

Comparative analysis of integrated and traditional security models

Traditional network security models are based on static mechanisms such as firewalls, IDS, and centralised access control systems. They apply rigidly defined rules and policies, which limit their ability to adapt to dynamic environments and multi-vector cyber-attacks. Static firewalls are efficient against known threats, but they are unable to respond quickly to new types of attacks or internal incidents. Centralised solutions control resources from a single location, but in large and distributed networks, response speed and performance are significantly reduced.

Integrated security models that combine AI, SDN, ZTA, and blockchain offer a more comprehensive approach. SDN provides centralised traffic flow management and dynamic routing, enabling rapid response to network changes. AI modules automatically analyse traffic, classify packets, detect anomalies, and predict potential threats in real time. ZTA provides adaptive access control and micro-segmentation, reducing the risks of internal threats, while blockchain ensures transparency and immutability of records, automating the audit and verification of user and device actions (Hashmi *et al.*, 2025).

A comparison of these two approaches reveals fundamental differences (Table 5). In traditional systems, incident response speed is limited by manual intervention, attack detection accuracy depends on predefined rules, and scalability and resilience to internal threats are significantly limited. Integrated models provide instant response thanks to AI and SDN, enable proactive detection of new and complex attacks, scale easily in multi-domain and cloud environments, and ensure comprehensive protection against internal and external threats through continuous access control and transparent auditing.

Table 5. Comparative analysis of traditional and integrated network security models

Parameter	Traditional models (static firewalls, centralised solutions)	Integrated models (AI + SDN + ZTA + blockchain)
Incident response speed	The response to events takes from a few minutes to hours; automation is limited to simple rules. For example, during a DDoS attack, manual traffic redirection	Reaction within a second thanks to AI that predicts attacks and SDN that dynamically redirects traffic. For example, AI detects traffic anomalies, and SDN changes routes to reduce load
Accuracy of attack detection	60-70% detection of known attacks; new threats are missed due to static signatures	90-95% thanks to the combined use of ML/DL for traffic analysis, ZTA behavioural patterns and log verification in blockchain
Scalability	Limited by centralised controllers, it is difficult to maintain multi-domain networks. Additional equipment and manual configuration are required for network expansion	High; SDN enables centralised management of thousands of switches, AI automatically adapts policies, and blockchain ensures log consistency across multi-domain systems
Resilience to internal threats	Low; control is limited by ACL rules or basic authorisations	High; ZTA continuously verifies users and devices, AI assesses risks in real time, and blockchain stores immutable records of all events
Transparency and audit	Limited by centralised logs, data modifications are possible in the event of server compromise	Complete transparency thanks to blockchain; all transactions are recorded, smart contracts automatically verify actions, and AI analyses logs for anomalies
Adaptability to dynamic changes	Non-existent; changes in topology, load or new threats require manual intervention	High: AI predicts traffic and threats, SDN dynamically changes routes, and ZTA adapts access rights in real time
Level of automation	Low; constant intervention by administrators is required to change rules, monitor and audit	Maximum; AI manages traffic classification, threat prediction, access policy adaptation, and blockchain provides automatic auditing without human intervention

Note: ACL – Access Control List
Source: compiled by the authors

The table shows that integrated security models significantly outperform traditional solutions in all key criteria. The advantage of integrated systems includes not only faster response to incidents and high accuracy in detecting attacks, but also the ability to perform automated audits, dynamic access control, and network infrastructure scaling. SDN enables centralised and efficient traffic flow management, AI predicts threats and adapts security policies, ZTA provides continuous user and device verification, and blockchain ensures transparency and immutability of records. Thanks to the synergy of these technologies, integrated models create an adaptive, resilient, and transparent network system capable of responding quickly to multi-vector threats and providing reliable protection for internal and external resources. Compared to classic static solutions, such integration can optimise resources, reduce response times, and increase the level of trust that users and administrators have in network security. At the same time, analysis of current publications confirms a common trend: a shift from static perimeter approaches to integrated architectures, where AI is responsible for threat analysis and prediction, SDN for dynamic traffic orchestration, ZTA for continuous access verification, and blockchain for transparent and immutable auditing. The results obtained are consistent with this vector and further emphasise the practical importance of explainable models, hybrid (on-/off-chain) logging schemes, and policy-as-code for closed-loop real-time control.

Conceptual overview of potential implementation cases for Ukraine and recommendations for optimising integrated network solutions

Ukraine has already formalised key elements of information security and digital trust management systems at the state sector level (Information Security Management System, qualified electronic trust services, centralised identification tools) and has direct experience in countering coordinated cyber operations against energy and telecommunications. Therefore, the next stage is the transition from perimeter-based, predominantly static models to "continuous verification" modes and policies that are data-driven and automatically applied through an SDN network factory in real time. The basis for such a transition is provided, on the one hand, by proven certification of IB processes in state organisations and services, and on the other hand, by mature open standards for state Zero-Trust transformations, which record control states of maturity by domains of identities, devices, networks, applications and data. Below is a conceptual overview of the possible application of these technologies in critical sectors of Ukraine (Table 6).

Table 6. Potential cases for Ukraine

Potential case	Technological components (AI, SDN, ZTA, Blockchain)	Expected result
Adaptive management of public electronic services	AI (anomaly detection, access control), integration with blockchain for data protection	Improved cyber resilience, minimised fraud, optimised service delivery processes
Protection of energy and telecommunications infrastructure	SDN (dynamic traffic management), AI (attack prediction), blockchain (transaction transparency, data protection)	Continuity of critical systems, reduction of cyberattack risks to power grids and mobile networks
Implementation of ZTA in multi-domain networks of state authorities	ZTA (Zero Trust), AI (automated user behaviour monitoring), blockchain (access auditing)	Reducing insider threat risks, securing access to resources, and controlling interdepartmental exchanges

Source: compiled by the authors

The first direction is aimed at modernising the portfolio of public e-services by integrating ZTA as an operational access "skeleton", SDN as a micro-segmentation and routing network factory, and AI as an analytical core for risk assessment and behavioural validation of requests. The organisational prerequisite is already in place: most state-owned enterprises were certified under the Information Security Management System according to ISO/IEC No. 27001 (2022), which formalises the Plan-Do-Check-Act (PDCA) cycle and standardises risk, incident and change management artefacts. In addition, the state segment of trust services is supported by the Central Certification Authority and qualified signature services, which simplifies the unification of trust roots and interagency interaction policies. On the technological level, this technology can be used to build a Zero-Trust gateway as a control plane that aggregates signals from proxies, identity gateways, and API brokers, correlates them in ML models, and then transmits them to the SDN controller for microsegmentation, Quality of Service (QoS) and routing policies based on subject context, resource sensitivity and current risk. Within the adjunct security bus, key events such as privilege escalations, behavioural profile deviations, and access policy changes are logged in a permissioned registry with minimal impact on transaction latency, creating a reproducible trail for compliance auditing and forensics. External benchmarks, from the Memorandum for the Heads of Executive Departments and Agencies (2022) to the DoD Zero Trust Strategy (2022), set specific control targets that can be used to build a roadmap for the maturity of the Ukrainian GovTech segment without the need to replicate already known approaches. As a result, this architecture puts the "user-service-data" interaction into a mode of constant verification and provides the basis for the "AI for Access Governance" pilot, in which XAI deterministically justify both an increase in the level of trust and the imposition of additional authentication factors.

The second case concerns energy and telecommunications and responds to the specifics of hybrid threats that combine targeted attacks on ICS segments with the destruction of public networks. Incidents involving the Industroyer/Industroyer2 family targeted energy network automation and demonstrated the ability to disrupt technological protocols, while in December 2023, a cyberattack on the largest mobile operator – Kyivstar – led to large-scale service disruptions comparable to "national-level failures" and demonstrated the need for policy-driven segmentation, domain isolation, and rapid recovery of controllability (Chuzavkov, 2023). The architectural response is that SDN deploys controllable overlays between the technology and business zones, while AI closes the feedback loop: it correlates telemetry from the core, transport and Radio Access Network segments, generates policy-as-code decisions and initiates the reconfiguration of routes, ACLs and QoS via the controller. For telecom operators, industry-proven virtualisation and automation programmes such as AT&T Domain 2.0 Vision White Paper (2013), Telefónica (2017), and LF Networking projects already describe target models with "closed control loops" where policies are formed based on event flow and applied automatically. For the energy sector, a relevant component is the constant auditing of commands and configuration changes through a permissioned registry. This approach has been verified in European pilots by Energy Web/TenneT to increase observability and reduce the cost of regulatory investigations. Together, this integration reduces detection and localisation time, increases the evidential value of operator and process attribution, and provides a "controlled degradation" mode during large-scale incidents through rapid isolation/segmentation scenarios.

The third vector is multi-domain networks of government agencies, where ZTA is the operational "constitution" of access, while SDN and AI provide the engine for real-time segmentation, orchestration, and policy adaptation. In practice, this implies the unification of trust roots, the federation of identity attributes between central and local authorities, the introduction of end-to-end visibility of access transactions, and the creation of service catalogues with clear separation of responsibilities in object-level access policies. For accelerated implementation, it is advisable to deploy in parallel an interagency trust mesh for transactional data exchange and an SD-WAN overlay for geographically dispersed institutions, where policies are propagated through ONAP-compatible interfaces and applied in the form of code, and all changes, from delegation of rights to temporary exceptions, are recorded in an immutable registry to simplify auditing and forensics. Methodological guidelines for government implementations are already available in the form of public Zero Trust strategies and analytics on cyber operations against

Ukraine, which emphasise the need to move from static standards to context-adaptive control modes. This can be used to form a step-by-step PDCA plan with milestones, metrics, and maturity profiles at the level of identity domains, devices, networks, and data. Combined with institutional support and professional clusters, this creates new opportunities for standardised deployments in the state's production circuits. A. Gupta *et al.* (2023) proposed the use of proxy smart contracts to implement Zero Trust principles in decentralised oracle networks. They explored how this approach enables secure data exchange between decentralised applications, minimising the risks of data manipulation or falsification. This correlates with the current conclusion about the role of blockchain as an integral layer of trust and audit, but the analysis by A. Gupta *et al.* of smart contract templates in the specific domain of DON does not cover the SDN network plane and micro-segmentation policies that were key in the model under consideration. The discrepancy is due to different system granularity.

In summary, these trajectories demonstrate that the integration of AI, SDN, and ZTA, with the measured use of blockchain as an immutable audit mechanism, forms an operational architecture capable of simultaneously accelerating detection and response, improving detection and attribution accuracy, scalable microsegmentation of service domains, and procedural transparency in security decision-making. The Ukrainian context, from proven certifications in the public sector and the compatibility of trust services to lessons learned from real cyberattacks against the energy and telecommunications sectors, provides both empirical grounds and practical markers of maturity for moving from pilots to systemic implementations, using open standards and industry roadmaps for network virtualisation and automation.

Optimisation of integrated network solutions requires a systematic approach that combines the development of technological infrastructure, human resources and international cooperation. The development of a national AI ecosystem is critical, as the implementation of AI Factory will enable the creation of autonomous cyber defence systems capable of responding quickly to new threats. The standardisation and integration of SDN, ZTA and blockchain technologies must be based on harmonisation with Ukrainian legislation and incorporate international compatibility and security requirements. Investing in training specialists is a priority, as the lack of qualified personnel is one of the main barriers to the development of comprehensive cybersecurity solutions. Lastly, international cooperation accelerates the implementation of new technologies and avoid duplication of efforts by using best practices and standards that have already been tested by other countries. To summarise the strategic directions for the development of the national cyber defence system, they have been systematised, correlating each benchmark with specific implementation mechanisms and expected results (Table 7).

Table 7. Recommendations and directions for their implementation

Direction	Specific implementation	Expected result
Development of the national AI ecosystem	Development of AI Factory, investments in data centres, creation of platforms for testing AI solutions	Autonomy, reduced dependence on external providers, and increased cyber resilience
Standardisation and integration of technologies	Development of national standards for SDN, ZTA, and blockchain integration; harmonisation with international standards	Ensuring compatibility, data protection, and adaptation to Ukrainian realities
Training and professional development of personnel	Certification programmes, creation of educational courses, partnerships with universities and international organisations	Formation of a highly qualified personnel reserve, reduction of personnel shortages
Cooperation with international partners	Participation in joint research, exchange of technologies, and creation of consortia in the field of cybersecurity	Acceleration of innovation, access to advanced technologies, and increased global integration

Source: compiled by the authors based on A. Kudriashov (2024)

Analysis of the table shows that the development of a national AI ecosystem through the creation of an AI Factory and corresponding data centres ensures autonomy and reduces dependence on external technology providers, while increasing the speed of anomaly detection and response to cyber threats. S. Mishra (2023) proposed a hybrid IDS system based on blockchain and ML to protect "smart" networks and maintain confidentiality. The system analyses traffic in real time, detects anomalies, and stores logs in a blockchain for transparent auditing. The results showed that the combination of ML and blockchain significantly improves attack detection efficiency while maintaining user data privacy. This is consistent with present findings on the feasibility of hybrid on-/off-chain approaches and AI analytics to ensure trust and reduce attack risks. The difference is in the level of application: in S. Mishra, IDS is the primary security tool, while in the present model, it is integrated into a broader Zero Trust perimeter alongside SDN and XAI. The standardisation and integration of SDN, ZTA and blockchain technologies ensures compliance with international standards and Ukrainian legislation, which can be used for the construction of a secure and flexible network architecture with minimal conflicts between different systems. Investments in training and certification of personnel create a highly qualified personnel reserve capable of effectively managing complex integrated systems, which is critical for

the stability of the national infrastructure. Active international cooperation accelerates innovation, the exchange of best practices, and access to advanced technologies, increasing the global integration and adaptability of Ukraine's cyber system. Overall, the table demonstrates a comprehensive approach in which technological, organisational, and human resources components are interrelated and mutually reinforce the effect of increasing cyber resilience.

A comprehensive approach to optimising integrated network solutions, where technological, organisational and human resources components are interconnected to enhance cyber resilience, is presented in Figure 4. The diagram illustrates the interaction between the development of the national AI ecosystem, the standardisation and integration of SDN, ZTA and blockchain technologies, investment in specialist training and international cooperation. It demonstrates how these areas support each other, creating an adaptive, scalable and secure network infrastructure capable of responding effectively to modern cyber threats and ensuring the resilience of state systems.

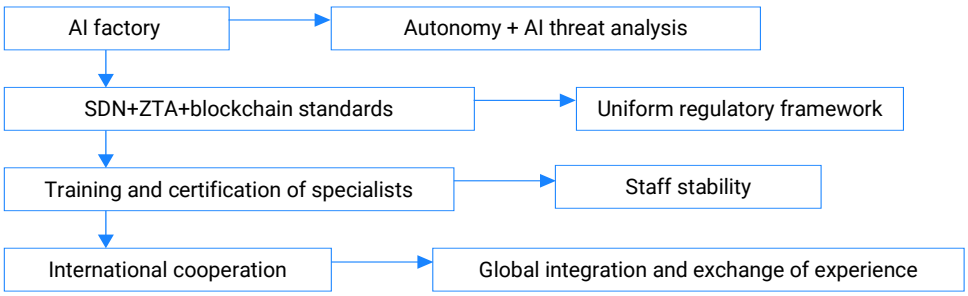

Figure 4. Optimisation of integrated network solutions
Source: compiled by the authors based on the data of H. Li *et al*. (2025)

Analysis of the diagram shows that successful optimisation of integrated network solutions is based on the synergy of technological, organisational and human resources components. The development of a national AI ecosystem ensures autonomy and rapid detection of anomalies, while the standardisation and integration of SDN, ZTA and blockchain guarantee the compatibility and security of the network infrastructure. Investments in staff training increase the level of expertise and readiness to respond to cyber incidents. International cooperation accelerates the implementation of advanced technologies and can be used to adapt best practices to the Ukrainian context. The diagram shows that the comprehensive combination of these elements creates an adaptive, scalable, and threat-resistant network architecture, where each component enhances the effectiveness of the others, providing a comprehensive system of state-level cyber protection.

In the doctoral thesis, C. Katsis (2025) developed a comprehensive framework for specifying, training, and implementing network-wide access control in Zero-Trust Network Architectures. The study described a methodology for building access policies, model training algorithms for dynamic control, and automated security enforcement mechanisms. The research confirmed that centralised policy specification combined with automated learning can improve scalability and security effectiveness in complex corporate networks. This is directly consistent with the current approach to policy-as-code and AI integration for automatic real-time rule updates. The difference is that C. Katsis emphasises the formalisation and modelling of policies, while the study also focuses on XAI and blockchain integration for auditing. The difference is due to the emphasis: theoretical foundation versus practical combination with transparency and accountability technologies. In turn, Z. Ajznblasm *et al.* (2025) considered AI-driven ZTA frameworks for large-scale dynamic networks using RL/behavioural models. Their study emphasises that combining AI and ZT makes cyber defence systems more adaptable and better able to respond to complex, multi-layered attacks. This is consistent with the current conclusion regarding the feasibility of a real-time AI policy engine.

Blockchain provides decentralised and immutable data storage. Each transaction on the network is recorded in blocks with cryptographic confirmation, which prevents unauthorised changes. Smart contracts automate event auditing and control of user and device actions, creating a transparent and reliable mechanism for accounting for all operations on the network (El Koshiry *et al.*, 2023). AI in Networking applies ML, DL, and RL methods. AI analyses traffic, classifies packets, detects anomalies, and optimises security policies. Models can predict potential threats, automatically change routing rules, and adapt access control in real time. AI is also capable of integrating data from blockchain to improve log reliability and ensure auditing (Ozkan-Okay *et al.*, 2024). A.S. Shah *et al.* (2025) reviewed AI- and blockchain-based clustering technologies for security in 6G networks. They described how combining AI for anomaly detection and blockchain for transparent data storage can create reliable clusters of secure nodes. Compared to other similar publications, their research highlights the significance of combining technologies to enhance the security of mobile and high-speed networks, particularly in the highly dynamic environment of 6G. Correlation with current results in distributed analytics and decentralised trust; potential non-correlation regarding the viability of full blockchain circuits under 6G URLLC

requirements. The present study proposed hybrid schemes (local edge solutions, asynchronous commit to the ledger), while some of the 6G scenarios in A. Shah *et al.* (2025) suggest an even higher level of "on-edge" autonomy with deferred auditing, a discrepancy caused by different latency SLAs and infrastructure maturity. In turn, S. Rahman & N. Perumath (2025) focused on Zero Trust management in the Internet of Things environment. This scoping review for IoT environments shows that the main barriers to Zero Trust are device identity, continuous attestation, and limited resources, requiring lightweight AI models and reduced cryptographic overhead. The results confirm these challenges and propose XAI and hybrid off-chain logs to reduce latency.

Overall, the study confirmed the effectiveness of integrated solutions in reducing incident detection time, improving attack attribution accuracy, reducing failure rates, and maintaining critical service availability at over 90%. Most of the results of the studies reviewed correlate with the current conclusion about the synergy of AI + SDN + ZTA + blockchain for adaptive protection: all authors agree on the need for continuous access validation, automated orchestration, and transparent logging. The presented contribution is complementary: it systematically combines the SDN network fabric with XAI, federated policy management, and hybrid blockchain auditing, and adds an applied implementation roadmap for Ukraine that bridges the gap between concept and operational implementation.

Conclusions

This study has demonstrated that the integrated application of Software-Defined Networking, Zero Trust Architecture, artificial intelligence, and blockchain constitutes a coherent and viable paradigm for next-generation secure network management. The analysis confirmed that each of these technologies performs a distinct yet complementary function: SDN enables centralised and programmatically controlled traffic management; ZTA implements continuous subject verification and access microsegmentation; AI provides traffic analysis, threat prediction, and automated adaptation of security policies; while blockchain establishes an immutable and transparent framework for auditing and trust. Their synergy makes it possible to overcome the key limitations of traditional perimeter-based security models that rely on static rules and fragmented control mechanisms.

The conceptual review and comparative analysis showed that integrated architectures significantly outperform traditional security models in terms of incident response speed, attack detection accuracy, adaptability to dynamic network conditions, resilience to insider threats, and auditability. The shift from static, rule-based protection to data-driven, policy-as-code, and closed-loop control systems enables real-time orchestration of security decisions across multi-domain and heterogeneous environments. In this context, AI-driven analytics combined with SDN-based traffic orchestration and ZTA-based access governance form the operational core of adaptive network defence, while blockchain strengthens accountability and trust through immutable logging and automated verification. The Ukraine-focused scenarios analysed in the study were deliberately framed as application-oriented conceptual implementations rather than empirical evaluations of named production networks.

These simulations – covering public electronic service platforms, critical energy and telecommunications infrastructure, and multi-domain government networks – illustrated the practical feasibility of applying integrated technologies under conditions of high threat intensity and organisational complexity. Drawing on peer-reviewed research and open policy and industry documents, the analysis demonstrated how such architectures can support continuous verification, rapid containment and recovery, and transparent post-incident analysis without reliance on proprietary datasets. This approach allowed the results to be generalisable and transferable while remaining sensitive to the specific security and governance context. At the same time, the study identified a number of structural limitations that must be addressed to ensure effective implementation. These include the explainability of AI-based decisions, the tension between adaptive learning mechanisms and the immutability of distributed ledgers, high computational demands, and the complexity of coordinating security policies across multiple administrative and technological domains. The proposed mitigation strategies, such as the use of Explainable AI, hybrid on-/off-chain logging schemes, model optimisation, and federated policy frameworks, provide a practical foundation for balancing automation, transparency, and performance.

The findings confirmed that integrated AI + SDN + ZTA + blockchain solutions represent not merely a technological upgrade but a strategic transformation of network security governance. For environments exposed to multi-vector cyber threats, including state-level digital services and critical infrastructures, such architectures enable a transition toward continuous, autonomous, and auditable security management. Future research should focus on experimental validation through controlled pilots, quantitative assessment of performance and resilience gains, and further refinement of explainability and interoperability mechanisms to support large-scale deployment in compliance with international standards.

Acknowledgements

None.

Funding

The study received no funding.

Conflict of Interest

None.

References

[1] Ajznblasm, Z., Deepika, A., Parameswaran, M., Satyanarayana, B., Srinivas, T., & Ramesh, P.S. (2025). Exploring Zero Trust artificial intelligence-based frameworks in large-scale dynamic networks for enhancing cybersecurity. In *Proceedings of the international conference on computational innovations and engineering sustainability* (pp. 1-7). Tamilnadu: IEEE. doi: 10.1109/ICCIES63851.2025.11032807.

[2] Alevizos, L., Ta, V.T., & Hashem Eiza, M. (2022). Augmenting Zero Trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, 5(1), article number e191. doi: 10.1002/spy2.191.

[3] Alhilali, A.H., & Montazerolghaem, A. (2023). Artificial intelligence based load balancing in SDN: A comprehensive survey. *Internet of Things*, 22, article number 100814. doi: 10.1016/j.iot.2023.100814.

[4] Alshehri, A., Tufekci, B., & Tunc, C. (2024). Identification management for Zero Trust through network analysis. In *Proceedings of the 21st international conference on computer systems and applications* (pp. 1-6). Sousse: IEEE. doi: 10.1109/AICCSA63423.2024.10912537.

[5] Aramide, O. (2022). Identity and access management (IAM) for IoT in 5G. *Open Access Research Journal of Science and Technology*, 5, 96-108. doi: 10.53022/oarjst.2022.5.2.0043.

[6] Aramide, O.O. (2024). Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems. *World Journal of Advanced Research and Reviews*, 23(3), 3304-3316. doi: 10.30574/WJARR.2024.23.3.2656.

[7] Ashfaq, F., Wasim, M., Shah, M.A., Ahad, A., & Pires, I.M. (2025). Enhancing security in 5G edge networks: Predicting real-time Zero Trust attacks using machine learning in SDN environments. *Sensors*, 25(6), article number 1905. doi: 10.3390/s25061905.

[8] AT&T Domain 2.0 Vision White Paper. (2013). Retrieved from https://www.att.com/Common/about_us/pdf/AT&T%20Domain%202.0%20Vision%20White%20Paper.pdf.

[9] Azam, Z., Islam, M.M., & Huda, M.N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. *IEEE Access*, 11, 80348-80391. doi: 10.1109/ACCESS.2023.3296444.

[10] Bashaa, M.H., Bhaya, W.S., & Al-aaraji, N.H. (2025). Integration of Zero Trust architecture and machine learning for improving the security of software defined networking: A review. *Journal of Intelligent Informatics, Networking, and Cybersecurity*, 1(1), article number 1. doi: 10.65445/3106-1192.1000.

[11] Batewela, S., Ranaweera, P., Liyanage, M., Zeydan, E., & Ylianttila, M. (2025). Addressing security orchestration challenges in next-generation networks: A comprehensive overview. *IEEE Open Journal of the Computer Society*, 6, 669-687. doi: 10.1109/OJCS.2025.3564788.

[12] Chaudhry, M. (2025). *A systematic mapping study on security challenges in software-defined cloud computing*. (Master's thesis, Åbo Akademi University, Turku, Finland).

[13] Chowdhury, B., Jahankhani, H., & Subramaniam, S. (2023). Zero-trust blockchain-based digital twin 6G AI-native conceptual framework against cyber attacks for e-healthcare. In H. Jahankhani & B. Issac (Eds.), *Cybersecurity and human capabilities through symbiotic artificial intelligence. ICGS3 2023. Advanced sciences and technologies for security applications* (pp. 453-479). Cham: Springer. doi: 10.1007/978-3-031-82031-1_23.

[14] Chuzavkov, S. (2023). Ukraine's largest mobile operator Kyivstar downed by "powerful" cyberattack. Retrieved from https://techcrunch.com/2023/12/12/ukraine-largest-mobile-operator-kyivstar-downed-by-powerful-cyberattack/?utm_source=chatgpt.com

[15] DoD Zero Trust strategy. (2022). Retrieved from https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

[16] Dwivedi, R., *et al*. (2023). Explainable AI (XAI): Core ideas, techniques, and solutions. *ACM Computing Surveys*, 55(9), article number 194. doi: 10.1145/3561048.

[17] El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M.Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain: Research and Applications*, 4(4), article number 100165. doi: 10.1016/j.bcra.2023.100165.

[18] Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., & Shabaz, M. (2023). Proxy smart contracts for Zero Trust architecture implementation in Decentralised Oracle Networks based applications. *Computer Communications*, 206, 10-21. doi: 10.1016/j.comcom.2023.04.022.

[19] Han, H., Liu, Z., Wang, X., & Li, S. (2021). Research of the relations among cloud computing, internet of things, big data, artificial intelligence, block chain and their application in maritime field. *Journal of Physics: Conference Series*, 1927, article number 012026. doi: 10.1088/1742-6596/1927/1/012026.

[20] Hashmi, E., Yamin, M.M., & Yayilgan, S.Y. (2025). Securing tomorrow: A comprehensive survey on the synergy of Artificial Intelligence and information security. *AI and Ethics*, 5(3), 1911-1929. doi: 10.1007/s43681-024-00529-z.

[21] ISO/IEC No. 27001. (2022). *Information security management systems*. Retrieved from https://surli.cc/mwmavy.

[22] Katsis, C. (2025). *End-to-end frameworks for the specification, learning and enforcement of network-wide access control in Zero-Trust Network Architectures*. (Doctoral thesis, Purdue University, West Lafayette, USA).

[23] Kudriashov, A. (2024). Artificial intelligence and security in 5G and 6G mobile technologies. *Computer-Integrated Technologies: Education, Science, Production*, 54, 236-242. doi: 10.36910/6775-2524-0560-2024-54-29.
[24] Latif, S.A., Wen, F.B., Iwendi, C., Wang, L.L., Mohsin, S.M., Han, Z., & Band, S.S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, 181, 274-283. doi: 10.1016/j.comcom.2021.09.029.
[25] Li, H., Xiao, M., Wang, K., Kim, D.I., & Debbah, M. (2025). Large language model based multi-objective optimization for integrated sensing and communications in UAV networks. *IEEE Wireless Communications Letters*, 14(4), 979-983. doi: 10.1109/LWC.2025.3529082.
[26] Malik, A., Arshid, K., Noonari, N., & Munir, R. (2025). Artificial intelligence-driven cybersecurity framework using machine learning for advanced threat detection and prevention. *Scholars Journal of Engineering and Technology*, 6, 401-423. doi: 10.36347/sjet.2025.v13i06.005.
[27] Memorandum for the Heads of Executive Departments and Agencies. (2022). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
[28] Mishra, S. (2023). Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy. *Electronics*, 12(16), article number 3524. doi: 10.3390/electronics12163524.
[29] Nagarjun, A.V., & Rajkumar, S. (2024). Exploring the potential of deep learning and blockchain for intrusion detection systems: A comprehensive review. *Journal of Circuits, Systems and Computers*, 33(16), article number 2430007. doi: 10.1142/S0218126624300071.
[30] Narayanan, S. (2025). AI-driven anomaly detection for telecom cloud security. *International Journal of Emerging Research in Engineering and Technology*, 25, 228-238. doi: 10.63282/3050-922X.ICRCEDA25-125.
[31] Nikitchenko, V.S. (2024). *Research on trends in the digital transformation of business structures based on Industries 4.0 and 5.0*. (Master's thesis, Sumy State University, Sumy, Ukraine).
[32] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEE Access*, 12, 12229-12256. doi: 10.1109/ACCESS.2024.3355547.
[33] Pemmasani, P.K., Gudepu, B.K., & Gonugunta, K.C. (2025). Unified AI command console for cybersecurity: Multi-AI integration with minimal manual intervention. *TechRxiv*. doi: 10.36227/techrxiv.174802397.73696913/v1.
[34] Rahman, S., & Perumath, N. (2025). *Implementing Zero Trust management in IoT environment-challenges and solutions: Scoping review*. Retrieved from https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1955680&dswid=-2231.
[35] Shah, A.S., Karabulut, M.A., Kamruzzaman, A., Alharthi, D., & Bradford, P.G. (2025). A survey on artificial intelligence and blockchain clustering for enhanced security in 6G wireless networks. *Computers, Materials & Continua,* 84(2), 1981-2013. doi: 10.32604/cmc.2025.064028.
[36] Speith, T. (2022). A review of taxonomies of explainable artificial intelligence (XAI) methods. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency* (pp. 2239-2250). New York: Association for Computing Machinery. doi: 10.1145/3531146.3534639.
[37] Svensberg, P. (2023). *Software-defined zero-trust network architecture: Evolution from Purdue model-based*. (Master's thesis, University of Turku, Turku, Finland).
[38] Telefónica. (2017). *Telefónica's UNICA architecture strategy for network virtualisation*. Retrieved from https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/03/Telefonica_Virtualisation_gCTO_FINAL.pdf.
[39] Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating artificial intelligence with Zero Trust architecture: Enhancing adaptive security in modern cyber threat landscape. *International Journal of Research and Analytical Reviews*, 9(2), 712-728.
[40] Vorokhob, M.V. (2023). *Models and methods for improving enterprise security policy based on the Zero Trust methodology*. (Doctoral thesis, Borys Grinchenko Kyiv University, Kyiv, Ukraine).

Синергія штучного інтелекту, SDN, Zero Trust та блокчейну: огляд нових тенденцій в безпечному управлінні мережами

Олександр Підпалий

Доктор філософії
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0009-0007-6852-7959

Олександр Романов

Доктор технічних наук, професор
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0002-8683-3286

Анотація. Дослідження є актуальним через потребу створення ефективних, прозорих і захищених від кібератак мережевих систем управління. Мета дослідження полягала у систематизації та критичному аналізі сучасних підходів до поєднання штучного інтелекту, програмно-конфігурованих мереж, архітектури Zero Trust та блокчейну для побудови адаптивних, прозорих і захищених від кібератак систем управління мережею. Проведено концептуальний огляд технологій безпечного управління мережею з застосуванням інтерпретативного та порівняльного аналізу наукових джерел, системного та структурно-категоріального аналізу характеристик вказаних технологій, моделювання сценаріїв їх застосування для підвищення адаптивності, прозорості та стійкості мережевих систем у критичних секторах України. Результати показали, що комбіноване використання цих технологій забезпечує централізоване управління трафіком, динамічну політику доступу, прозорість операцій та здатність до автономного виявлення загроз, значно підвищуючи стійкість мережі до багатовекторних кібератак. Виявлено, що основними проблемами інтеграції цих технологій у мережевих системах є непрозорість рішень штучного інтелекту, конфлікти між динамічністю моделей та незмінністю блокчейну, високі вимоги до ресурсів і складність узгодження політик у мультидоменних мережах. Впровадження Explainable Artificial Intelligence, гібридних архітектур, off-chain рішень, оптимізації моделей та федеративних протоколів дозволило подолати обмеження, забезпечуючи прозору, адаптивну та безпечну мережеву систему, здатну ефективно реагувати на загрози та динамічні зміни середовища. Доведено, що традиційні рішення, засновані на статичних фаєрволах та централізованому контролі, обмежені у швидкості реагування, точності виявлення атак та масштабованості. Інтегровані моделі, що поєднують штучний інтелект, програмно-конфігуровані мережі, архітектури Zero Trust та блокчейну, забезпечують миттєве реагування на загрози, високоточне виявлення атак, динамічний контроль доступу, автоматизований аудит та ефективне масштабування, створюючи адаптивну, стійку та прозору мережеву систему. Результати дослідження можуть бути використані для розробки й оптимізації політик кібербезпеки, автоматизації контролю доступу та моніторингу мережевих подій, а також для побудови масштабованих і прозорих архітектур систем управління

Ключові слова: мережева безпека; кіберзахист; виявлення вторгнень; машинне навчання; explainable artificial intelligence