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

Information Technologies and Computer Engineering **Vol. 22, No. 1. 2025**

Article's History: Received: 10.12.2024 Revised: 03.03.2025 Accepted: 24.04.2025

UDC 004.7 DOI: 10.63341/vitce/1.2025.55

Integration of Zero Trust and Blockchain in SDN networks: An overview of threats and methods of their elimination

Oleksandr Pidpalyi*

Postgraduated Student
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, Professor
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 purpose of the study was to identify theoretically sound methods for integrating Zero Trust and blockchain concepts to improve the overall security of software-defined networks (SDN). The research was based on the development of a theoretical network model that includes an SDN controller, switches, routers, and hosts, which used virtualisation tools such as GNS3, VirtualBox, and Docker. The theoretical basis of the study covered the analysis of key threats, including DDoS attacks, routing manipulation, insider threats, attacks on the application programming interface (API), and specific vulnerabilities of blockchain consensus mechanisms. Simulation scenarios were developed to demonstrate the potential impact of these threats on the security and performance of SDN networks. Analysis of the results obtained theoretically confirmed that the use of Zero Trust policies significantly reduces the risks of insider attacks and improves the protection of the SDN controller due to the principles of constant access verification and micro-segmentation. Integration of blockchain technologies increases the reliability of routing and traffic management, preventing malicious interference in the network infrastructure. Theoretical methods for authentication and verification of requests using blockchain significantly improve the protection of APIs and interaction interfaces. In addition, hybrid consensus algorithms have shown the potential to improve network performance and ensure its resistance to attacks. The study highlighted the importance of integrating Zero Trust and blockchain as an effective solution for eliminating a wide range of threats in SDN networks. This opens up new prospects for the protection of telecommunications systems and lays the theoretical foundation for further research and improvement of security methods. The practical significance of the study is to develop specific recommendations for implementing a comprehensive SDN security system based on blockchain technologies and Zero Trust principles. The proposed solutions can be used both in the public sector to protect critical infrastructure and in the private sector to ensure the security of corporate networks

Keywords: access control; data verification; risk reduction; distributed systems; attack resistance; communication security

Introduction

The rapid development of information technologies creates new challenges for managing network resources. Conventional network management methods are losing effectiveness due to increasing infrastructure complexity, increasing data volumes, and increased cyber threats. The urgency of introducing innovative network management technologies for Ukraine is conditioned by the critical need for modernisation of telecommunications infrastructure.

Suggested Citation:
Pidpalyi, O., & Romanov, O. (2025). Integration of Zero Trust and Blockchain in SDN networks: An overview of threats and methods of their elimination. *Information Technologies and Computer Engineering*, 22(1), 55-68. doi: 10.63341/vitce/1.2025.55

*Corresponding author

In the context of digital transformation of the economy and increasing global information risks, it is necessary to ensure reliable protection of information systems and compliance with international security standards. Blockchain technologies and the Zero Trust concept offer modern mechanisms for improving network security. They allow implementing the principles of decentralised data protection, constant verification of access and minimising the risks of compromising information resources. The introduction of these approaches creates a new paradigm of network security, which is critical for ensuring national information infrastructure and competitiveness in the global digital environment. This leads to a high interest from the scientific community.

Research by X. Guo *et al*. (2022) and W. Li *et al*. (2020) emphasised the importance of software-defined networks in modern telecommunications, emphasising their role in providing flexible network management and traffic optimisation by separating the control plane from the data plane. This architectural feature provides unprecedented flexibility, but at the same time creates new security challenges, in particular, due to the centralised nature of the SDN controller, which becomes vulnerable to DDoS attacks, routing manipulation, insider threats, and attacks on the application programming interface (API). In this context, the integration of blockchain technologies can significantly improve SDN security by decentralising management, which eliminates the risks associated with a single point of failure.

The consensus mechanisms used in the blockchain allow creating a distributed and reliable platform for verifying changes in routing or security policies, reducing the likelihood of successful attacks on the controller. In addition, the blockchain helps to ensure the integrity and immutability of data by storing change logs in network policies, which becomes an effective tool for countering insider threats. According to J.A. Fadhil & S.R. Zeebaree (2024), blockchain, as a decentralised technology, can be used to manage traffic and authenticate data, providing protection against external interference. The use of blockchain to authenticate data to SDN not only ensures its reliability, but also creates a platform for transparent traffic management, which is crucial for countering complex cyber threats. Integration of this technology reduces the risk of unauthorised interference, even in the event of attacks on centralised network elements.

K. Gai *et al*. (2019) in their research presented the concept of differentiated privacy based on blockchain for ensuring the security of the industrial Internet of Things (IoT). The concept of blockchain-based differentiated privacy can be adapted for SDN networks, where data protection at the level of each network node is important. This reduces the risk of confidential information leakage, especially in environments with an increased number of IoT devices. Y. Xu *et al*. (2019) further developed this idea by offering a blockchain-based network computing service scheme with non-consistency. K. Gai *et al*. (2022) proposed a blockchain-based access control scheme to ensure reliable data exchange between organisations in the Zero Trust paradigm. The proposed blockchain-based access control scheme reinforces the Zero Trust paradigm, as it provides authentication at every stage of data exchange. This is especially important for SDN networks, where the absence of a single point of trust is a key element of security.

P. Zheng *et al*. (2023) further highlighted the possibilities of using blockchain technology in the development of decentralised applications, which allows creating a transparent access control system. Such applications contribute to effective traffic monitoring and rapid detection of anomalies, which allows quickly identifying security threats based on blockchain records. An additional layer of security is the integration of the Zero Trust approach, which provides for constant verification of each action or access, regardless of the internal or external status of the user. X. Yan & H. Wang (2020) emphasised that Zero Trust is based on the principle of minimal trust and constant access verification, which significantly increases the network's resilience to insider threats. In addition to increasing resistance to internal threats, Zero Trust integration allows creating a detailed access structure that minimises the risks of network compromise due to privacy or integrity violations. This approach works effectively in conditions of high dynamics of the network environment, in particular in cloud services.

SDN allows dynamically managing real-time access policies, supported by the blockchain to securely store these policies and counteract their substitution. The Zero Trust architecture combined with SDN allows for network micro-segmentation, isolating critical resources from potentially dangerous areas, and the blockchain supports this process, ensuring transparency and resilience to change. In addition, the integration of blockchain identification allows increasing the level of verification of devices and users within the framework of the Zero Trust concept, creating comprehensive protection of the network infrastructure. Thus, the combination of SDN, blockchain and the Zero Trust approach paves the way for creating adaptive, threat-resistant and secure network environments that meet the challenges of the modern world.

Ukrainian researchers have contributed to the investigation of the possibilities of integrating blockchain into telecommunications systems. O. Bykonia & N. Romanovska (2024) noted that the integration of Zero Trust and blockchain can significantly improve the security level of critical infrastructure, help to reduce the risks of cyber-attacks and ensure compliance with international standards. Their proposed blockchain-based computing service scheme helps to increase the resilience of SDN networks to failures through decentralised data storage and the use of smart contracts. This ensures reliable operation of networks even if individual nodes are compromised.

Existing SDN security studies have identified several significant gaps. Firstly, while SDN provides high flexibility in managing network infrastructure, the centralised nature of controller management creates significant

vulnerabilities, particularly in relation to DDoS attacks, routing manipulation, API attacks, and internal threats. Secondly, conventional security management methods often do not meet the requirements of modern dynamic and distributed environments, because they are based on the assumption of trust in internal users and devices. Thirdly, blockchain and Zero Trust technologies are considered separately in the context of various security aspects, which limits their potential for comprehensive solutions to problems in SDN networks.

Given these gaps, the purpose of this study was to develop practical recommendations for integrating Zero Trust concepts and blockchain technology to improve SDN security. The study included the creation of a theoretical model of the SDN network using virtualisation tools; investigation of the possibilities of implementing Zero Trust Principles to protect against insider threats; development of methods for applying blockchain technologies to ensure the integrity and reliability of data.

Materials and Methods

The research methodology was based on a comprehensive analysis of threats to SDN and the study of the capabilities of Zero Trust and blockchain technologies to neutralise detected threats. The main task was to create a methodology that considers the features of decentralisation and strict access control inherent in these technologies to improve the overall sustainability of the network. At the initial stage of the study, a theoretical analysis of the main threats in SDN networks was carried out. Attention was focused on threats related to unauthorised access, attacks on the control and management layers, internal threats and possible compromises of the centralised controller. The potential impact of these threats on the functioning and integrity of SDN networks was studied separately.

The following methods were chosen to develop the integration approach: hierarchical threat analysis, blockchain-based identification analysis, and multi-factor authentication methods typical of Zero Trust. The method of hierarchical threat analysis helped to structure threats by risk levels, which became the basis for determining the necessary counteraction measures. This ensured consistency in the choice of protection methods, which was the basis for developing an effective security model. The blockchain was used as the basis for decentralised storage of access and transaction data, which provided increased transparency and protection against data forgery. This solution is a key to eliminating centralised points of failure. Instead, Zero Trust methods were implemented to dynamically manage access to network resources based on the minimum trust principle, which helped to consider constantly changing access conditions (Dhiman *et al.*, 2024).

Simulation of SDN networks with blockchain and Zero Trust integration was implemented using tools such as GNS3, VirtualBox, Docker, and Python libraries for network analysis. The OpenDaylight SDN controller was used for modelling, which provided interaction between switches and other network components in a virtual environment. When developing the model, the need to implement micro-segmentation principles specific to the Zero Trust concept was considered, which included constant verification of each transaction and access request.

To build the model, three segments of the SDN network were used, each of which had a different access level to ensure the isolation of critical resources from potentially dangerous areas. The blockchain was used to record and verify transactions, and provide transparency and protection against unauthorised changes. Proof of Stake was chosen as the consensus algorithm, which reduced the computational load compared to conventional approaches such as Proof of Work. Several key scenarios were identified for modelling attacks, including DDoS attacks with an intensity of up to 10,000 requests per second, API compromises, and internal threats related to credential leaks.

Three different attack scenarios were modelled to evaluate the effectiveness of the proposed approach in conditions as close to real-life as possible. Scenario 1 involved an attack using social engineering techniques; Scenario 2 – an attack using social engineering techniques and hacking of network components; Scenario 3 – a combined attack that simultaneously uses social engineering techniques, hacking of network components and exploits vulnerabilities in communication protocols. A multi-level approach to threat analysis was implemented, which included identifying early signs of a potential attack, assessing its likely impact on the network, and making quick decisions to neutralise it through an adaptive response system that automatically regulates access to network resources depending on the threat level. The adaptive response system provided the ability to automatically adjust access depending on the threat level. This helped to counteract combined attacks more effectively, considering both internal and external threats.

The process of integrating Zero Trust and the blockchain included creation of a conceptual model of interaction between SDN network components. This model covered steps from identifying potential threats to defining access control methods and creating a transparent access accounting mechanism using the blockchain. To reduce the network load, a hybrid blockchain was chosen, where some of the data was processed centrally, and mission-critical transactions were recorded in the blockchain.

Validation of the approach using a simulation model of the SDN network with integration of Zero Trust and blockchain allowed to empirically confirm the advantages of the proposed solution. The main evaluation criteria were response time, protection from external threats, resistance to internal attacks, and overall support costs. The comparison was carried out with conventional security methods, such as network segmentation, which provided division into separate logical segments, reducing the risks of uncontrolled spread of attacks, and centralised authentication (RADIUS or TACACS+), which controls access to resources using centralised credential verification servers.

Results

Security threats and implementation model of Zero Trust and blockchain in SDN networks

Threat analysis for SDN was a key stage of research aimed at identifying weaknesses in the security mechanisms of these systems. The main threats to SDN networks can be characterised by their impact on the network and the level of risk. Among the main threats were unauthorised access, attacks on the control layer, internal threats, and compromise of the centralised controller. Unauthorised access poses a serious threat to data privacy and the stability of network operations, especially if attackers exploit vulnerabilities in interaction via the API. Remote attacks are aimed at gaining uncontrolled access to network resources. They have a high level of risk because attackers can seize control of critical network components. Control layer attacks, such as DDoS attacks, are critical because this layer is responsible for managing all processes on the network. Their consequences may include significant failures or a complete shutdown of the network infrastructure. Data theft, which is also a critical threat, threatens privacy and can lead to significant financial and reputational losses, especially in cases of working with confidential information. Internal threats that arise as a result of compromising the credentials of privileged users can lead to manipulation of routes or changes in data configurations, causing serious damage to network security. Internal threats that arise from the use of privileged access are difficult to detect. Their level of risk is high because they allow manipulating data and network configurations. Data interception is characterised by an average level of risk and is fraught with leakage of confidential information, which is critical in some industries (Guo *et al*., 2022). Special attention should be paid to the problem of a centralised controller, which in the conventional SDN architecture is a single point of failure. Compromising this element creates the risk of uncontrolled traffic redirection or loss of access to the entire network. In addition, attackers can use combined attacks, combining social engineering, exploiting communication protocol vulnerabilities, and compromising network components. This highlights the need for a multi-level approach to protection that can respond to different types of threats in a complex way. Threat analysis also helps to determine priority countermeasures (Table 1).

Table 1. Main threats to SDN networks and how to eliminate them using Zero Trust and blockchain

Threat	Impact on the network	Risk level	Elimination methods
Remote attacks	Uncontrolled access to network resources	High	Verification of each request, two-factor authentication
Attacks on the central controller	Network failures due to management violations	Critical	Use of blockchain to decentralise controller functions
Data theft	Violation of privacy and reduced trust	Critical	Cryptography, secure access under Zero Trust principles
Internal threats	Use of privileged access	High	Continuous monitoring and segmentation of the network, use of blockchain
Data interception	Leak of confidential information	Moderate	Traffic encoding, segmented access

Source: created by the authors based on X. Guo *et al*. (2022), J. Li *et al*. (2022), S. Ghasemshirazi *et al*. (2023)

Attacks on the central controller and data theft pose the greatest risk, while data interception is one of the less critical threats. To counter these threats, it is recommend using the Zero Trust approach, which provides for constant monitoring and verification of access, regardless of the source of the request. This reduces the risk of both internal and external threats. Additionally, the integration of blockchain technology ensures decentralised management, transaction transparency, and makes it impossible to modify data without authorisation. Such measures allow eliminating major vulnerabilities and ensuring reliable network protection. Blockchain adds a level of transparency, eliminating data forgery and reducing the risk of unauthorised modifications. The integration of artificial intelligence (AI) technologies with Zero Trust and blockchain in SDN networks creates a strong foundation for the development of innovative solutions in the field of cybersecurity, which will allow organisations to effectively counter modern threats and provide reliable protection of critical information infrastructure in the face of the constant evolution of cyber threats.

The conceptual model of interaction between SDN network components was developed to analyse the integration of Zero Trust and the blockchain to ensure a high level of security and performance. The schematic image shows the SDN network architecture, which includes integration of Zero Trust and blockchain technologies. The central component of the system is the SDN controller, which performs network management functions, makes routing decisions, and controls access to network resources. The controller interacts with switches, routers, and end nodes (hosts), providing data exchange. Switches and routers provide data transmission in accordance with the policies set by the controller, and hosts are the sources and consumers of traffic (Fig. 1).

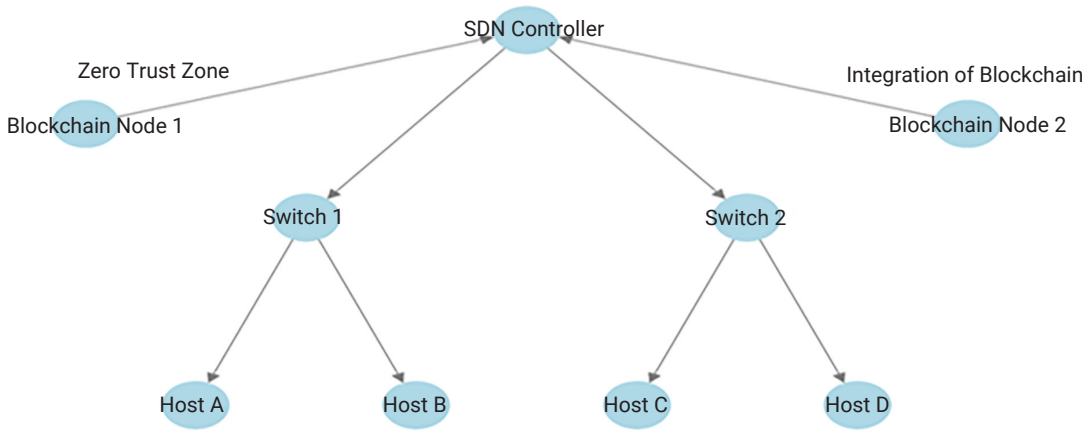

Figure 1. Schematic representation of an SDN network with integration of Zero Trust and blockchain technologies
Source: created by the authors

The model also integrates blockchain and Zero Trust technologies to improve security. Blockchain is used for decentralised storage of access logs and changes in network policies, providing transparency and protection against data forgery. The Zero Trust concept is implemented through multi-level authentication and strict control of each access, regardless of the source. This isolates critical resources from potentially dangerous areas and significantly reduces the risks of internal threats. The image also shows key relationships between components: the SDN controller interacts with the blockchain, passing access policy data for writing to the distributed ledger. Switches are connected to the end nodes (hosts) through which traffic is transmitted, and the blockchain provides control and verification of all transactions. The process of interaction in the model covers the stages from identifying potential threats to creating a transparent access accounting mechanism. Access policies are based on the principles of minimal trust, and authentication takes place at every level, which allows effectively responding to threats and preventing unauthorised actions.

The results of the study showed that using a layered architecture can significantly reduce the load on the network and improve its performance. In particular, this approach allows distributing the processing of different types of transactions or data between individual levels of the system, reducing competition for computing resources. In a layered architecture, the lower levels may be responsible for processing basic requests, while the upper levels focus on critical operations such as authentication or performing smart contracts. This method has proven effective for large corporate and government SDN networks with high bandwidth, where the volume of traffic and the number of users is constantly growing (Bykonia & Romanovska, 2024). Based on the layered structure, it was possible to achieve greater flexibility and stability of the system, and reduce delays in performing key operations. Thus, the proposed approach allows adapting Zero Trust and blockchain to the specific needs of large networks, while maintaining a high level of security and transparency.

The integration of Zero Trust and blockchain creates a new security paradigm that can effectively counter modern threats. Continuous monitoring of access and decentralisation of management ensures a high level of trust in information circulating on the network. These technologies significantly increase the transparency of access, reduce the risk of unauthorised changes, and create an additional layer of protection, especially against attacks on centralised network elements. The blockchain was chosen for decentralised storage of event and transaction logs, which provides transparency and protection against data forgery. The Zero Trust concept aims to constantly monitor and verify access to resources, regardless of the source of the request. This approach allows creating a detailed model of access policies based on the principles of "never trust, always verify" (Liu *et al*., 2020). The combination of Zero Trust with blockchain technology provides additional decentralisation and transparency and allows recording all transactions in a distributed ledger. This eliminates data forgery and reduces the risk of unauthorised network interference.

Model testing: Description of attack scenarios and security system responses

To test and validate the model, two SDN network configurations were created: a conventional security model and a model that integrated Zero Trust and blockchain. The conventional model was based on network segmentation, which provided a division into separate logical segments, reducing the risks of uncontrolled spread of attacks, and centralised authentication (RADIUS or TACACS+), which controlled access to resources using centralised credential verification servers. The model with Zero Trust and blockchain complemented these approaches with modern security principles, such as continuous verification of users and devices, minimisation of access privileges, micro-segmentation to restrict access, transparent logging of all events in the blockchain, and distributed verification of access transactions, which ensured the detection of unauthorised changes in the network. The effectiveness of both configurations

was evaluated in a simulation environment, where real-world attack scenarios were modelled, including social engineering techniques, hacking network components, and exploiting vulnerabilities in communication protocols.

In the first scenario, the attack was based on social engineering techniques. The attacker sent a phishing email to the SDN network administrator with a request to confirm access to the system through the "official portal". After entering their credentials, they were contacted by an attacker who tried to gain access to the SDN controller. A conventional security system was able to detect abnormal activity only after an attacker entered, without identifying the source of the compromise. In turn, the system with the blockchain and Zero Trust blocked access due to multi-factor authentication, and also recorded all access attempts in the blockchain for further analysis.

The second scenario combined social engineering and hacking of network components. An attacker obtained administrator credentials through phishing, and then changed the switch configuration to redirect traffic through the server they controlled. In this case, the conventional system detected anomalies in routing after the compromised traffic reached the attacker. A system with a blockchain and Zero Trust detected the threat earlier, as it required multi-level authorisation to make configuration changes. The request was blocked, and all actions of the attacker were recorded in the blockchain.

The third scenario combined social engineering techniques, hacking network components, and exploiting vulnerabilities in communication protocols. The attacker first obtained administrator credentials, then changed the router settings and entered vulnerable code into protocols, which led to a DoS-type attack and partial network paralysis. The conventional security system detected an attack only after significant failures occurred, and identifying the source of the compromise remained a difficult task. The system with the blockchain and Zero Trust blocked the request to change the protocol in a timely manner due to multi-level access verification. All attempts to make changes, including details of the entered code, were recorded in the blockchain, which helped to quickly isolate the problem and prevent further compromise (Table 2).

Table 2. Comparison of the response of a conventional system and a system with blockchain and Zero Trust

Scenario	Attack type	Conventional system response	System response with blockchain and Zero Trust
1	Social engineering	Partial detection after compromise, source not identified	Blocking unauthorised access, logging in the blockchain
2	Social engineering + compromise	Delay in detecting routing anomalies	Blocking routing changes, transparent logging
3	Social engineering + compromise + protocol exploitation	Inability to respond quickly to a combination of attacks	Detection at all stages through multi-factor and blockchain consensus

Source: created by the authors based on X. Guo *et al*. (2022), W. Li *et al*. (2020), S. Ghasemshirazi *et al*. (2023)

According to the conducted research, the integration of Zero Trust and the blockchain helped to achieve a significantly higher level of security compared to standard security measures. A special feature of this approach was that during the compromise of one of the network elements, the blockchain recorded all historical data of changes, which prevented further expansion of the attack due to the transparency and immutability of records. Zero Trust provided constant control of access to resources based on the principle of "never trust, always verify", regardless of whether this refers to internal or external users of the network. The results of model validation for indicators such as network operation latency, connection stability, access transparency, and threat mitigation are presented in Table 3.

Table 3. Validation results

Indicator	Conventional model	Zero Trust + Blockchain
Scenario 1		
Network operation delay	5-7 ms	10-15 ms
Connection stability	95%	98%
Transparency of access	60%	100
Ability to counter threats	40%	98%
Scenario 2		
Network operation delay	6-10 ms	12-18 ms
Connection stability	70%	95%
Transparency of access	50%	100%
Ability to counter threats	40%	98%
Scenario 3		
Network operation delay	7-12 ms	15-25%
Connection stability	50%	92%
Transparency of access	40%	100%
Ability to counter threats	20%	96%

Source: compiled by the authors

The validation results demonstrated significant advantages of integrating Zero Trust and blockchain technologies over the conventional model. In the context of network operation latency, the conventional model was faster, providing minimal latency values due to its simple architecture (5-7 ms in the first scenario, 6-10 ms in the second, 7-12 ms in the third). However, the integration of Zero Trust and blockchain, which added consensus and access verification mechanisms, led to an increase in latency (10-15 ms, 12-18 ms, and 15-25%, respectively), which is a justified compromise for improving security. The performance score is shown in the delay comparison graph between the conventional system and the integrated model, which clearly shows a trade-off between improving security and increasing response time (Fig. 2).

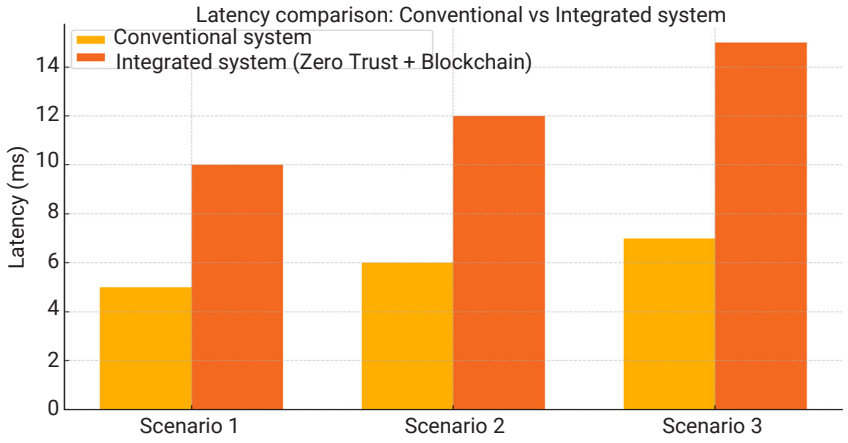

Figure 2. Comparison of delays between a conventional system and an integrated model (Zero Trust + Blockchain) for three scenarios

Source: created by the authors

The stability of connections in the conventional model remained high only under normal conditions (95% in the first scenario), but significantly decreased to 70% in the second and 50% in the third scenarios during attacks. In turn, the model with integration of Zero Trust and blockchain showed significantly higher stability of connections: 98% in the first, 95% in the second, and 92% in the third scenario. This was achieved by restricting access only for authorised users and ensuring that the network is resistant to threats (Fig. 3).

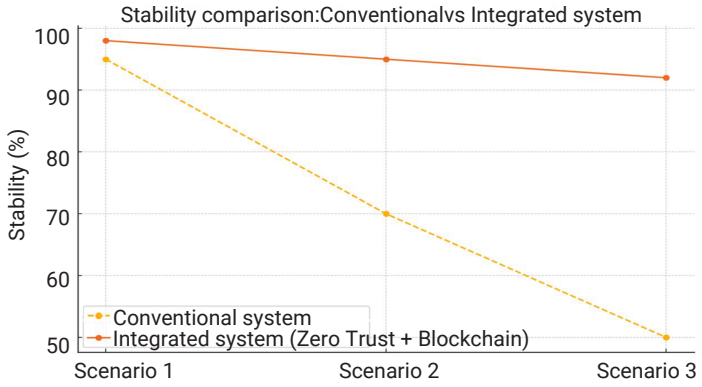

Figure 3. Comparison of connection stability between a conventional system and an integrated model (Zero Trust + Blockchain) in three scenarios

Source: created by the authors

Access transparency in the conventional model is limited (40-60%), as event logs may be incomplete or changeable. In the blockchain model, transparency reaches 100% because all operations are recorded unchanged, which ensures full control and audit of all actions in the network. The ability to counter threats in the conventional model was quite low (40% in all scenarios), which is explained by the lack of modern protection mechanisms. Instead, the integration of Zero Trust and blockchain increased this figure to 98%, protecting the network from unauthorised access and hacking of logs. The combination of these technologies allows quickly detecting and neutralising even complex attacks.

Overall, the integration of Zero Trust and blockchain has shown significant advantages. Access transparency reached its maximum level (100%), the ability to counteract threats was 96-98%, and the stability of connections remained high

even in difficult conditions. A slight increase in the latency of network operations is justified by an increase in the level of security, transparency, and reliability. These results confirm the feasibility of implementing such technologies to create a secure and sustainable cloud environment.

One of the key advantages of Zero Trust and blockchain in SDN networks is enhanced security through control of each transaction and decentralised protection. This allows creating a self-contained system where all transactions are recorded and verified, which makes it difficult to fake or make unauthorised changes. The disadvantages of this approach include an increase in network load, in particular, due to the processing of blockchain transactions, which leads to increased latency and resource consumption. In addition, the Zero Trust approach requires significant resources to authenticate and verify each user and request. A comparison of the conventional approach to security and the Zero Trust and blockchain-based approach is presented in Table 4.

Table 4. Comparison of the conventional approach to security and the approach based on Zero Trust and blockchain

Indicator	Conventional approach	Zero Trust + Blockchain
Centralisation of management	Central management	Decentralisation through blockchain
Protection against internal threats	Limited	In-depth control of each access
Transparency	Limited	High, due to the blockchain
Network load	Low	High, due to additional checks
Delay	Minimum	Moderate, depending on the volume of checks
Implementation cost	Relatively low	High, given the support resources

Source: created by the authors based on K. Gai *et al*. (2022), P. Dhiman *et al*. (2024), O. Bykonia & N. Romanovska (2024)

The analysis shows that the use of Zero Trust and blockchain in SDN networks is effective, but requires optimisation and resource management to reduce costs and delays. Potential scenarios for using the integrated model are particularly relevant for environments with high security requirements, in particular, in the context of possible combined attacks. Due to the transparency and immutability of data, blockchain is extremely effective in environments where a high level of trust in information is important. This applies to such industries as public administration, financial services, critical infrastructure (in particular, energy), healthcare, etc. The simulation results confirmed that the integration of Zero Trust and blockchain technologies can significantly reduce risks, increase transparency, and ensure control over network transactions. The implementation of Zero Trust in such networks provides protection against suspicious activity, internal threats and privacy violations, while the blockchain adds another layer of security, recording all changes and actions on the network. This approach opens up opportunities for creating autonomous networks that are much less dependent on centralised controllers and provide the maximum level of reliability and protection.

Challenges and limitations of implementing Zero Trust and blockchain in SDN networks

The implementation of Zero Trust and blockchain in SDN networks is accompanied by a number of challenges that cover technical, resource, and organisational aspects. One of the key limitations of implementing blockchain and Zero Trust technologies in SDN networks is the high requirements for memory and computing resources. This is conditioned by the need to store a large amount of data in the blockchain, which is accompanied by significant computing costs, especially in large networks with high bandwidth. The complexity of blockchain protocols and the constant access verification typical of Zero Trust further complicate the situation. In such networks, CPU and memory resources must process a huge number of requests, which leads to increased response times and creates delays that are critical for systems with high efficiency requirements.

In addition, the scalability of such systems becomes a challenge due to the need to dynamically manage large volumes of traffic and maintain operational efficiency even under high load conditions. This requires the introduction of hybrid approaches and automation of security policies to reduce the load on the system. However, even under such conditions, high computational costs remain a significant problem that requires further optimisation. Delays in performing operations are one of the key limitations of integrating blockchain and Zero Trust technologies. They arise from continuous access verification, consensus processes, and transaction control, which adds additional steps to each transaction. This can significantly affect network performance, especially in systems with high operational requirements, such as financial transactions or critical infrastructure management. This problem is compounded in large networks with a large number of users and devices, where manual administration of Zero Trust policies becomes time-consuming and error-prone. Process automation is necessary to reduce delays and increase efficiency, in particular, the introduction of adaptive systems and machine learning. This allows dynamically adjusting access policies based on the context and user behaviour, and minimise the impact of delays on network performance.

Another challenge is scalability: integrating blockchain and Zero Trust into large corporate or government SDN networks can become problematic due to significant amounts of data that require storage and processing. This requires the development of dynamic resource scaling methods to maintain efficient network performance even under high load conditions (Liu *et al*., 2020). Data privacy is also an important limitation. Despite the fact that the blockchain ensures the immutability of data, it also makes all transactions available for viewing, which can lead to a

potential leak of confidential information. S. Ghasemshirazi *et al*. (2023) noted that in such cases, it is necessary to develop secure storage methods where the blockchain is combined with other cryptographic methods to provide the necessary level of data protection.

The complexity of implementing technologies is also a serious barrier. It is caused by the need for significant changes in the architecture of SDN networks, in particular, reconfiguring controllers, creating new access policies, and scaling the blockchain infrastructure for processing large amounts of data. The use of Zero Trust and blockchain technologies in SDN networks requires significant financial investments, especially at the initial stages of implementation. The main items of expenditure are the purchase and configuration of computing resources necessary to maintain blockchain operations and ensure reliable multi-level authentication. As the network scale and traffic volumes increase, the cost of processing and storing data increases, as each transaction requires authentication. However, despite the high costs, this approach can be cost-effective for companies that need reliability and security.

In addition, managing Zero Trust policies on large networks with a large number of users and devices is becoming increasingly difficult. High interaction dynamics require constant monitoring, updating access policies, and detecting anomalies, which is complicated by the growing scale of the network. This makes manual administration extremely time-consuming and potentially error-prone. Automating processes using adaptive systems and machine learning technologies can partially solve these problems. This will allow dynamically adjusting access policies based on analysis of user and device behaviour, reducing the amount of manual work and improving management efficiency. However, even such solutions require additional investment in the development and implementation of the appropriate infrastructure.

Recommendations for integrating Zero Trust concepts and blockchain technology in SDN networks

Integration of Zero Trust and blockchain into SDN networks requires a comprehensive approach that considers architectural, technical, and organisational aspects. The first step is to analyse the network infrastructure to identify its critical assets, potential vulnerabilities, and specific needs. This information is the basis for developing a hybrid architecture that combines decentralised blockchain solutions for mission-critical data and centralised ones for less significant operations. To implement the Zero Trust approach, it is necessary to implement network micro-segmentation, which will ensure the isolation of critical areas from potentially dangerous ones. It is recommended to use multi-level authentication, which includes risk factors such as location, device type, and user behavioural patterns. Dynamic access control should automatically adjust policies based on changes in the network environment and user behaviour. Blockchain should be used to increase the transparency of access control. All access transactions and policy changes must be recorded in a distributed ledger, which ensures that they remain unchanged and can be audited. The implementation of smart contracts will automate the management of access policies and ensure a quick response to potential threats. To protect the API, it is important to implement request tokenisation and distributed identification mechanisms.

To avoid the high costs and delays associated with computing, it is recommended to implement modern consensus mechanisms, such as Proof of Stake, and optimising network performance through caching and prioritising requests. Automated monitoring using AI technologies can significantly improve the effectiveness of security management, helping to quickly detect anomalies and adapt the system to new threats. Successful integration requires not only technical solutions, but also organisational support. Staff should be trained to effectively manage new systems. In addition, security policies should be updated regularly to meet the latest threats and technology changes. Effective implementation of Zero Trust and blockchain involves creating a step-by-step integration plan that includes pilot projects, testing the system in real-world conditions, and scaling it. At all stages, implementation performance should be evaluated, including response time, stability, performance, and security level analysis.

In addition, it is important to develop mechanisms for resilience to new threats, considering the specifics of the industry or organisation. For example, in high-risk environments (finance, critical infrastructure), additional security mechanisms should be integrated, such as transaction-level data encryption or mandatory audit of all accesses. Compliance with these recommendations will create an SDN network that not only provides a high level of security, but is also flexible, adaptive to changes and resistant to modern cyber threats.

Discussion

The integration of the Zero Trust architecture and blockchain platform implemented in this study demonstrates significant potential for improving the security, transparency, and reliability of SDN networks. The proposed approach provides effective protection of network resources through a combination of strict access control, decentralised data storage, and automation of security policies. The use of blockchain enabled the creation of an immutable log of transactions and events, which increases transparency and simplifies auditing. Moreover, the implementation of Zero Trust provided isolation of critical resources and dynamic access control, which significantly reduces the risks of internal and external threats. The analysis showed high efficiency of the proposed approach even in conditions of large networks with high bandwidth and a significant number of users. However, key challenges were considered, in particular, delays in performing operations and high computing costs, which allowed optimising integration using hybrid solutions and modern consensus mechanisms. Thus, the results of this study confirmed the possibility of

scaling the proposed technologies and their practical value for use in complex corporate and government networks.

The architecture that uses blockchain to manage security in SDN for 5G applications is presented in the paper by D. Das *et al*. (2023). The researchers considered methods for protecting communications in 5G environments through the use of blockchain as a means for authentication and storage of records. The results of the study showed that the introduction of blockchain can significantly improve the security of communications by reducing the risks of unauthorised access and data compromise. The researchers proposed the integration of blockchain smart contracts for authentication management, which allowed automating access verification and providing a transparent data storage mechanism. This solution has proven to be particularly effective for high-traffic environments such as 5G, reducing the risk of data loss even in the event of attacks on network nodes.

A comparison with the results obtained in the study shows similarities in the approach to ensuring transparency and decentralisation of access control. In the current study, blockchain was also used to strengthen the security of software-defined networks (SDNs) by recording transactions and automating authentication processes. The same technology using blockchain to improve digital security in the defence sector was proposed by O. Semenenko *et al.* (2024), noting its effectiveness in protecting data from cyber threats.

In this study, the integration of Zero Trust and blockchain to improve the security of SDN networks showed high efficiency in minimising risks and preventing unauthorised access, but this was accompanied by significant computational costs and delays, in particular, due to the constant authentication of each request. As stated by L. Alevizos & V.T. Ta (2024), cybersecurity automation capabilities using AI, blockchain, and smart contracts can be used to solve these problems. The researchers proposed approaches that combine AI for monitoring and predicting threats with blockchain smart contracts for automating access policies. This allows only quickly responding to detected threats, but also provides adaptive resource management in real time. For example, AI can analyse network traffic to identify anomalies, and smart contracts can automatically restrict access in the event of a potential threat. The main challenge is the need to balance blockchain transparency, responsiveness, and computing costs. In the current paper, the main focus is on using a hybrid blockchain to minimise the load, but using AI to predict and automate threat detection, as indicated by L. Alevizos & V.T. Ta, opens up new opportunities for optimising Zero Trust systems. In addition, the use of AI can reduce delays in decision-making, since instead of static security rules, it is possible to implement dynamic models that adapt to new attack scenarios. This makes their approach more promising for scenarios with high threat dynamics, such as in cloud or financial networks.

Features of implementing Zero Trust in cloud networks were discussed by S. Ahmadi (2024). The researcher discussed current challenges and potential areas for developing Zero Trust technology to ensure data security in the cloud environment. Managing Zero Trust policies for a large number of users and devices can be challenging. This problem can be partially overcome by automating access control processes using machine learning and adaptive systems. D. Ajish (2024) examined the role of AI in Zero Trust technologies, in particular, its ability to improve security in the architecture. The researcher analysed how AI helps to detect anomalies, assess access risks, and automate security policy management processes. Due to machine learning algorithms, AI can dynamically adapt to changes in the network environment, quickly respond to new threats, and reduce the human factor in decision-making. AI also helps to automate the access verification process by using behavioural analysis to create user and device profiles. This helps to more accurately determine the level of trust and adapt access rights accordingly. In addition, AI is actively used to monitor network traffic in real time, which allows quickly detecting attempts to compromise or violate access policies.

S. Dhar & I. Bose (2020) explored the possibilities of using blockchain and Zero Trust to protect IoT devices. The researchers proposed an architecture that provides reliable access control and data protection in the IoT. In industrial IoT networks used to monitor and manage production processes, Zero Trust and blockchain can significantly improve system security by preventing unauthorised access to devices and reducing the risk of data manipulation. The decentralised blockchain architecture makes such networks less vulnerable to centralised attacks, and Zero Trust provides control at the level of individual devices.

A. Kulkarni *et al*. (2024) investigated the use of blockchain and physically unclonable functions to protect Field-Programmable Gate Array supply chains. This system uses Zero Trust to ensure the authenticity of components and the security of information exchange between manufacturers and suppliers. The researchers created a model based on the uniqueness of the physical characteristics of each device, which provides identification without the need to store sensitive data on the device. The blockchain in this architecture is used to capture transactions and ensure their immutability, creating a reliable platform for interaction between supply chain participants. The proposed approach provides a high level of security, since the combination of blockchain and physically unclonable functions reduces the risk of component tampering or unauthorised interference in the delivery process. Using Zero Trust adds another layer of protection, because access to components is possible only after multi-level authentication, which minimises the likelihood of compromise even in the presence of insider threats. Compared to conventional supply chain security methods, such as centralised certification systems, this approach is more transparent and reliable, since the blockchain ensures the immutability of data about each transaction, and physically unclonable functions guarantee the authenticity of each physical component.

Compared to the current study, which focused on integrating Zero Trust and blockchain to protect SDN networks, approach of A. Kulkarni *et al*. focused on the physical security of devices and supply chains. Although both approaches demonstrate effectiveness in providing security, their challenges are similar: increasing system load and delays due to decentralisation and multi-level authentication.

A blockchain-based infrastructure for providing Zero Trust models on peripheral computing devices was proposed in the paper by C. Bicer *et al*. (2023). The researchers described the concept of using blockchain to improve device security and data transmission at the edge of the network without having to trust a central administrator. The security benefits of Zero Trust and blockchain may exceed performance limits, but for large-scale networks, there is a need to improve consensus and data processing mechanisms. For example, hybrid blockchain solutions can be used to improve efficiency, where basic data is processed centrally and critical transactions are stored on the blockchain. This allows reducing the load on the network, while maintaining a high level of security.

A blockchain-based authentication scheme for railway networks was proposed by Y. Feng *et al*. (2023). The researchers considered the features of ensuring the security of communications in the railway infrastructure using Zero Trust. Together, they provide reliable protection against a wide range of attacks, especially relevant for modern dynamic network environments. Compared to other approaches, such as network segment encryption and role-based access control, Zero Trust and blockchain offer an additional layer of protection by constantly monitoring and recording all transactions. This makes them indispensable for environments where privacy and trust in data are critical.

Using proxy smart contracts to implement Zero Trust in decentralised oracles networks, as suggested in the paper by A. Gupta *et al*. (2023), is an example of the benefits of integrating these technologies. Such smart contracts allow strictly controlling access to data and transactions in oracles' networks, which is crucial for ensuring security. Integration of Zero Trust with blockchain smart contracts ensures transparency of interaction, since each transaction is recorded in an immutable register. This eliminates the risks associated with data manipulation and reduces the likelihood of compromise even in the event of internal threats. In addition, smart contracts automate access verification processes and the implementation of security policies, which significantly increases the efficiency and speed of the system.

Z. Bassfar *et al*. (2023) proposed a Zero Trust architecture using quantum device identification. The study focused on ensuring the security of network access through quantum technologies. Integration with machine learning tools for adaptive access control will allow faster detection of anomalies, automate the process of managing access policies, and increase the efficiency of the Zero Trust environment. In addition, the use of a hybrid blockchain model, where some information is processed centrally, and critical transactions are stored in a decentralised network, can provide faster data processing while maintaining a high level of security.

Zero Trust architecture automation solutions were investigated by Y. Cao *et al*. (2024). The researchers considered the advantages and problems associated with process automation in Zero Trust. In their research, they focused on using automated access policies that adapt in real time depending on changes in user behaviour or system status. This is achieved through the integration of AI-based analytics, which provides monitoring and detection of threats, and automatic changes to security policies without the participation of an administrator. The results of the study showed that Zero Trust automation significantly increases the effectiveness of threat detection and reduces risks associated with the human factor. For example, in networks with a large volume of traffic or many users, automation can reduce delays that occur due to manual access control. In addition, AI can identify complex attacks that may be invisible to conventional monitoring systems. Automated solutions also allow considering the context (location, device, request time), which is important for building more flexible and secure networks. This is especially true for critical infrastructures or financial SDN networks, where data security is critical. However, as the researchers note, automation also has problems, in particular, related to scalability and the potential complexity of configuring such systems. They point out the need for a combination of automation and transparency that can provide more sustainable and productive Zero Trust networks. Their results support the feasibility of recommendations in the work on AI integration for dynamic access control in environments with high security requirements.

Conclusions

The integration of Zero Trust and blockchain concepts into SDN networks has demonstrated high efficiency in improving security, access transparency, and network resilience to threats. Analysis of the results confirmed that the introduction of multi-level access control, micro-segmentation, and transparent policy management significantly reduces the risk of compromise from both internal and external attacks. The implemented model using the blockchain ensured the immutability of records and reduced the risk of data manipulation, which helped to achieve 96-98% effectiveness of countering threats compared to conventional security methods.

Integration of the Zero Trust architecture and blockchain technology into SDN networks was evaluated as an effective strategy for countering detected threats. Zero Trust provides continuous access verification, reducing the risk of unauthorised actions, especially by internal users. Each element of the network requires authentication and authorisation for access, which minimises the possibility of an attack. Blockchain technology adds a level of decentralisation and transparency, which avoids dependence on a single control centre and prevents data forgery. The blockchain also registers all transactions and

changes in the network, which creates a reliable mechanism for monitoring and auditing.

As a result of the analysis of the main threats to software-defined networks (SDN), it was found that the greatest danger is represented by attacks on the control and management layers. In particular, common threats include unauthorised access to network resources, attacks on a centralised controller, data leaks, and internal threats. These threats significantly affect the security and stability of SDN networks, undermining their integrity and confidentiality. It was found that conventional approaches are not always able to provide an adequate level of protection, since they rely on centralised management, which is vulnerable to external attacks.

The results confirm that the use of Zero Trust and blockchain significantly increases the stability of SDN networks even in high-risk environments, ensuring connection stability and minimising downtime. The use of a hybrid blockchain has reduced the load on the network, while maintaining a high level of security. Despite the slight increase in network latency due to multi-level access verification, the advantages of network transparency and security outweigh these disadvantages. Analysis of the results showed that the use of Zero Trust and blockchain contributes to a significant increase in the level of security in SDN networks, but simultaneously increases the requirements for computing resources and network delays. Further research on methods for optimising blockchain protocols is recommended, in particular, the use of consensus mechanisms with lower resource consumption, such as Proof of Stake, instead of Proof of Work. It is also important to consider integrating machine learning to automate access control and real-time threat detection. This will not only increase efficiency, but also reduce the need for manual intervention.

Promising areas of future research are improving system scalability and reducing delays by optimising blockchain architectures, in particular, the introduction of multi-level models and the development of hybrid models, where the main data is processed centrally, and mission-critical transactions are stored on the blockchain. This approach will help to reduce network load and provide the necessary level of security.

Acknowledgements

None.

Funding

The study received no funding.

Conflict of Interest

None.

References

[1] Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, 26(2), 215-228. doi: 10.9734/jerr/2024/v26i21083.

[2] Ajish, D. (2024). The significance of artificial intelligence in Zero Trust technologies: A comprehensive review. *Journal of Electrical Systems and Information Technology*, 11(1), article number 30. doi: 10.1186/s43067-024-00155-z.

[3] Alevizos, L., & Ta, V.T. (2024). Automated cybersecurity compliance and threat response using AI, blockchain & smart contracts. *International Journal of Information Technology*, 17, 767-781. doi: 10.1007/s41870-024-02324-9.

[4] Bassfar, Z., Sayeed, A., Bala, P., Alshehri, A., Alanazi, M., & Zubair, S. (2023). Toward secure and resilient networks: A Zero-Trust security framework with quantum fingerprinting for devices accessing network. *Mathematics*, 11(12), article number 2653. doi: 10.3390/math11122653.

[5] Bicer, C., Murturi, L., Donta, P.K., & Dustdar, S. (2023). Blockchain-based Zero Trust on the edge. *ArXiv*. doi: 10.48550/arXiv.2311.16744.

[6] Bykonia, O., & Romanovska, N. (2024). Perspectives of the development of the information and communication technologies sector in Ukraine. *Scientific Bulletin of International Association of Scientists. Series Economy Management Security Technologies*, 3(1). doi.org/10.56197/2786-5827/2024-3-1-8.

[7] Cao, Y., Pokhrel, S.R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of Zero Trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, 21(10), 294-317. doi: 10.1007/s11633-023-1456-2.

[8] Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., & Biswas, U. (2023). Blockchain enabled SDN framework for security management in 5G applications. In *ICDCN 23: proceedings of the 24th international conference on distributed computing and networking* (pp. 414-419). New York: Association for Computing Machinery. doi: 10.1145/3571306.3571445.

[9] Dhar, S., & Bose, I. (2020). Securing IoT devices using Zero Trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, 31(1), 18-34. doi: 10.1080/10919392.2020.1831870.

[10] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K.U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of Zero Trust network model. *Sensors*, 24(4), article number 1328. doi: 10.3390/s24041328.

[11] Fadhil, J.A., & Zeebaree, S.R. (2024). Blockchain for distributed systems security in cloud computing: A review of applications and challenges. *Indonesian Journal of Computer Science*, 13(2), 1576-1605. doi: 10.33022/ijcs.v13i2.3794.

[12] Feng, Y., Zhong, Z., Sun, X., Wang, L., Lu, Y., & Zhu, Y. (2023). Blockchain enabled Zero Trust based authentication scheme for railway communication networks. *Journal of Cloud Computing*, 12(1), article number 62. doi: 10.1186/s13677-023-00411-z.

[13] Gai, K., She, Y., Zhu, L., Choo, K.W., & Wan, Z. (2022). A blockchain-based access control scheme for Zero Trust cross-organizational data sharing. *ACM Transactions on Internet Technology*, 23(3), article number 38. doi: 10.1145/3511899.

[14] Gai, K., Wu, L., Zhu, L., Zhang, Z., & Qiu, M. (2019). Differential privacy-based blockchain for industrial internet-of-things. *IEEE Transactions on Industrial Informatics*, 16(6), 4156-4165. doi: 10.1109/TII.2019.2948094.

[15] Ghasemshirazi, S., Shirvani, G., & Alipour, M.A. (2023). Zero Trust: Applications, challenges, and opportunities. *ArXiv*. doi: 10.48550/arXiv.2309.03582.

[16] Guo, X., Wang, C., Cao, L., Jiang, Y., & Yan, Y. (2022). A novel security mechanism for software defined network based on blockchain. *Computer Science and Information Systems*, 19(2), 523-545. doi: 10.2298/CSIS210222001G.

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

[18] Kulkarni, A., Hazari, N.A., & Niamat, M.Y. (2024). A Zero Trust-based framework employing blockchain technology and ring oscillator physical unclonable functions for security of field programmable gate array supply chain. *IEEE Access*, 12, 89322-89338. doi: 10.1109/ACCESS.2024.3418572.

[19] Li, J., Lv, H., Lei, B., & Xie, Y. (2022). A consensus approach for SDN controllers based on blockchain. In *CSSE '22: proceedings of the 5th international conference on computer science and software engineering* (pp. 170-174). New York: Association for Computing Machinery. doi: 10.1145/3569966.3570015.

[20] Li, W., Meng, W., Liu, Z., & Au, M.-H. (2020). Towards blockchain-based software-defined networking: Security challenges and solutions. *IEICE Transactions on Information and Systems*, E103.D(2), 196-203. doi: 10.1587/transinf.2019INI0002.

[21] Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., & Choo, K.-K. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, 166, article number 102731. doi: 10.1016/j.jnca.2020.102731.

[22] Semenenko, O., Kirsanov, S., Movchan, A., Ihnatiev, M., & Dobrovolskyi, U. (2024). Impact of computer-integrated technologies on cybersecurity in the defence sector. *Machinery & Energetics*, 15(2), 118-129. https://doi.org/10.31548/machinery/2.2024.118.

[23] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. *IEEE Transactions on Industrial Informatics*, 15(6), 3632-3641. doi: 10.1109/TII.2019.2897133.

[24] Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In X. Sun, J. Wang & E. Bertino (Eds.), *Artificial intelligence and security* (pp. 50-60). Singapore: Springer. doi: 10.1007/978-981-15-8083-3_5.

[25] Zheng, P., Jiang, Z., Wu, J., & Zheng, Z. (2023). Blockchain-based decentralized application: A survey. *IEEE Open Journal of the Computer Society*, 4, 121-133. doi: 10.1109/OJCS.2023.3251854.

Інтеграція Zero Trust і Blockchain у SDN-мережах: огляд загроз та методів їх усунення

Олександр Підпалий

Аспірант
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 спрямоване на визначення теоретично обґрунтованих методів інтеграції концепцій Zero Trust і Blockchain з метою підвищення загальної безпеки програмно-конфігурованих мереж (SDN). Дослідження базувалося на розробці теоретичної моделі мережі, яка включає в себе SDN-контролер, комутатори, маршрутизатори та хости, для чого було використано інструменти віртуалізації, такі як GNS3, VirtualBox та Docker. Теоретична основа дослідження охоплює аналіз ключових загроз, серед яких DDoS-атаки, маніпуляції з маршрутизацією, інсайдерські загрози, атаки на application programming interface (API), а також специфічні уразливості механізмів консенсусу Blockchain. Імітаційні сценарії були розроблені для демонстрації потенційного впливу цих загроз на безпеку та продуктивність SDN-мереж. Аналіз отриманих результатів теоретично підтверджує, що застосування політик Zero Trust суттєво знижує ризики інсайдерських атак і покращує захист SDN-контролера завдяки принципам постійної перевірки доступу і мікросегментації. Інтеграція технологій Blockchain підвищує надійність маршрутизації та управління трафіком, запобігаючи спробам зловмисного втручання в мережеву інфраструктуру. Теоретичні методи аутентифікації та верифікації запитів з використанням Blockchain значно покращують захист API та інтерфейсів взаємодії. Крім того, гібридні алгоритми консенсусу показали потенціал для підвищення продуктивності мережі та забезпечення її стійкості до атак. Проведене дослідження підкреслює важливість інтеграції Zero Trust і Blockchain як ефективного рішення для усунення широкого спектра загроз у SDN-мережах. Це відкриває нові перспективи для захисту телекомунікаційних систем і закладає теоретичну основу для подальших досліджень і вдосконалення методів безпеки. Практична значимість дослідження полягає у розробці конкретних рекомендацій щодо впровадження комплексної системи захисту SDN на основі технологій блокчейн та принципів Zero Trust. Запропоновані рішення можуть бути використані як у державному секторі для захисту критичної інфраструктури, так і в приватному секторі для забезпечення безпеки корпоративних мереж

Ключові слова: контроль доступу; верифікація даних; зниження ризиків; розподілені системи; стійкість до атак; безпека комунікацій