ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.45 doi: 10.32620/reks.2026.2.16

**Oleksandr PIDPALYI[1], Oleksandr ROMANOV[1], Larysa GLOBA[1], Anton ROMANOV[2], Mykola NESTERENKO[3]**

*[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine*
*[2] National University «Kyiv Aviation Institute», Kyiv, Ukraine*
*[3] Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine*

# iTZBEI: AN INTEGRAL SECURITY METRIC FOR SDN ARCHITECTURES INTEGRATING ZERO TRUST AND BLOCKCHAIN

***The subject matter of the article is*** *the iTZBEI (Integrated Trust–ZTA–Blockchain SDN Efficiency Index) – a novel composite metric for quantitative security assessment of software-defined networks (SDN) integrating Zero Trust Architecture (ZTA) and Blockchain technologies. The relevance of the research is determined by the fact that the centralized SDN control model generates critical vulnerabilities, including DDoS attacks, unauthorized routing manipulation, and insider threats – for which no unified quantitative evaluation framework currently exists.* ***The study introduced*** *a formalized aggregated security metric that enables continuous monitoring and comparative assessment across all components of the SDN–ZTA–Blockchain architecture.* ***The tasks to be solved include:*** *(1) identification of principal SDN attack vectors; (2) formalization of a transaction-processing algorithm covering the full access lifecycle; (3) definition of nine local security indicators; and (4) construction of the iTZBEI index with justified weighting coefficients.* ***The methods used*** *combine mathematical formalization of access control processes, cryptographic transaction verification, and experimental emulation of attack scenarios in a Mininet–OpenDaylight–Hyperledger Fabric environment.* ***Conclusions.*** *The obtained results of the article consist in the development of a functional algorithm that performs dynamic verification of user requests, makes adaptive authorization decisions according to the principles of least privilege, and records these decisions in an immutable distributed ledger. A metrics system is proposed, including local indicators such as the Continuous Authorisation Integrity Score (CAIS), the Blockchain Audit Integrity Score (BAIS), and the Local Policy Integrity (LPI). On this basis, the generalized Integrated Trust and Zero-Trust Blockchain Evaluation Index (iTZBEI) is described as an aggregated metric for comparative evaluation and continuous monitoring of the network's security state.* ***Scientific novelty.*** *This study introduces a unified SDN + ZTA + Blockchain framework for network security, formalizes a transaction-level algorithm that directly links access decisions with distributed audit procedures, and proposes the iTZBEI metric as the first integral indicator for evaluating the integration's effectiveness in dynamic network environments.*

**Keywords***:* ***SDN security, Zero Trust, Blockchain, security metrics, authorisation integrity, iTZBEI, audit systems****.*

## 1. Introduction

Modern telecommunications infrastructures increasingly rely on Software-Defined Networking (SDN) as a foundational architecture for centralized traffic management, flexible routing, and separation of control and data planes. While these properties simplify policy enforcement and network programmability, the centralized control model simultaneously introduces critical vulnerabilities. A compromised SDN controller, a denial-of-service attack targeting the control plane, or unauthorized manipulation of routing rules can affect the entire network infrastructure simultaneously - a risk profile fundamentally different from traditional distributed architectures [1].

In this study, the threat landscape for SDN environments encompasses four principal attack categories confirmed through experimental simulation. DDoS attacks targeting the SDN controller cause complete loss of network availability through controller overload. Control plane attacks enable the unauthorized modification of routing rules, redirecting traffic through malicious nodes. Data plane attacks allow the interception and manipulation of network traffic. Finally, insider threats originating from compromised authorized nodes are particularly difficult to detect under conventional perimeter-based security models. Each category was modeled under controlled conditions to assess the vulnerability of unprotected SDN infrastructure and the effectiveness of the proposed countermeasures.

To address these risks, Zero Trust Architecture (ZTA) enforces continuous verification of every access request regardless of origin, while Blockchain provides a cryptographically secured, immutable audit ledger that

eliminates single points of failure in logging and policy enforcement [2, 3]. Their combination with SDN - referred to as the SZB architecture - creates a layered security framework in which centralized network management, dynamic access control, and tamper-proof auditing operate as a coordinated system.

### 1.1. Motivation

Despite growing research interest in SZB-type architectures, a fundamental gap remains: no existing work proposes a unified quantitative metric for evaluating the overall security effectiveness of SDN–ZTA–Blockchain integration. Existing metrics are either local in scope - reflecting only a single component, such as authorization latency or transaction throughput – or lack the formal structure necessary for continuous monitoring and cross-configuration comparison.

This makes it impossible to assess whether an SZB system is operating effectively as an integrated whole, or to identify which specific component is degrading overall security performance. This paper addresses that gap by introducing iTZBEI (Integrated Trust–ZTA–Blockchain SDN Efficiency Index) - a composite, dimensionless security metric that aggregates nine local indicators across both the ZTA and Blockchain layers into a single weighted index.

## 1.2. State of the art

Prior works have addressed individual components of SZB-type integration. A risk-based access control engine for IoT environments was proposed in [4], enabling adaptive authorization decisions, but without addressing SDN-specific challenges such as controller latency or policy scalability. A Blockchain-based Zero Trust mechanism for 6G networks [5] achieves fine-grained security through inner-product encryption, yet lacks integration with programmable SDN controllers. Decentralized access control for smart grids [6] demonstrates improved enforcement efficiency, but omits flow-level monitoring and SDN coordination. Blockchain-enabled ZT for underwater sensor networks [7] emphasizes energy efficiency but does not address SDN orchestration or integral evaluation metrics.

Broader state-of-the-art reviews confirm this fragmentation, showing that most efforts to augment Zero Trust with Blockchain remain endpoint- or component-centric and stop short of SDN-level orchestration [8].

At the SDN layer, previous studies [9, 10] have highlighted the potential of SDN for adaptive network management and its inherent vulnerabilities. Previous studies [13, 14, 15] have demonstrated that combining blockchain with ZTA principles enables dynamic policy management and immutable access logging, while smart contracts further automate policy verification and reduce human-factor risk [16]. Complementary studies have formalized SDN control-plane decision logic and developed mathematical models of controller behavior that underpin the transaction-level formalization adopted in this study [11, 12]. At the consensus layer, dedicated Blockchain consensus schemes for SDN controllers have been proposed to reduce coordination overhead [17], while energy-aware consensus protocols address the resource constraints typical of IoT and edge deployments [18].

The analysis confirms that while significant progress has been made in individual domains, no existing work formalizes a transaction-level algorithm or introduces a comprehensive integral metric for continuous security evaluation of unified SDN–ZTA–Blockchain systems. The present work directly addresses this limitation.

An earlier overview by the authors [19] qualitatively surveyed these threats and mitigation approaches; the present paper substantially extends this analysis by formalizing the transaction-level algorithm and introducing the quantitative iTZBEI index.

### 1.3. Objectives and tasks

This study aims to design a formalized security assessment framework for the SZB architecture and introduce iTZBEI as its integral evaluation metric. The SZB architectural solution presents the integrated framework's three-layer structure. The SDN layer encompasses the application, control, and data planes: SDN applications and the ZTA Policy Management Module operate at the application plane, while the SDN controller, which acts as the central decision point, manages traffic through the Northbound and Southbound interfaces, coordinating OpenFlow-based switches at the data plane level. The ZT layer implements continuous access verification through the Policy Enforcement Point (PEP), which includes a policy-processing module, trust-score evaluation, and authorization-status tracking. Context-aware decisions are supported by external Policy Inputs, including SIEM, PKI/IAM, Threat Intelligence, and ML analytics, collected via the Context Collector and end-node agents. The Blockchain layer serves as the logical level of auditing and verification, maintaining an immutable register of policies and decisions through the Verification and Logging module. The interaction between layers follows three types of flows: data traffic, traffic control signals, and safety/audit signals, ensuring full traceability of every access decision from initiation to distributed logging.

To achieve this, the following tasks are addressed: (1) identification of principal attack vectors and security limitations of conventional SDN mechanisms; (2) development of a formalized transaction-processing algorithm covering the full access lifecycle; (3) definition of nine local security indicators, each mapped to a specific phase of the algorithm; and (4) construction of the iTZBEI aggregated index with justified weighting coefficients enabling quantitative, comparative, and

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

continuous security monitoring. The SZB architectural solution (Fig.1.) shown below:

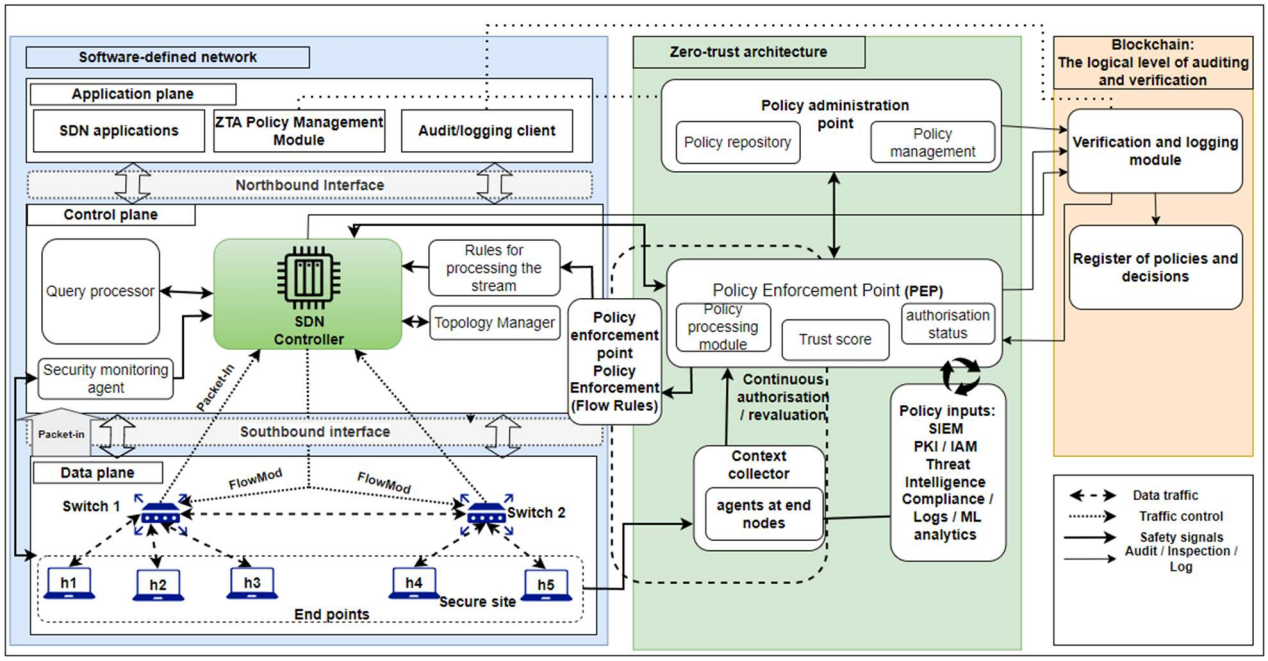


Figure 1. Architectural overview of the SZB framework: interaction between SDN control and data planes, Zero Trust policy enforcement components, and Blockchain-based auditing and verification layer.

The remainder of this paper is structured as follows. Section 2 presents the formalized transaction-processing algorithm for the SZB architecture, covering the full access lifecycle from initial SDN request through Zero Trust authorization to Blockchain audit logging. Section 3 describes the experimental setup, including the Mininet-based SDN emulation, OpenDaylight controller, and Hyperledger Fabric deployment. Section 4 introduces the nine local security indicators and derives the iTZBEI aggregated index with its weighting methodology. Section 5 presents and discusses the experimental results. Section 6 concludes the paper and outlines directions for future research.

## 2. Materials and methods of research

### 2.1. Functional algorithm for processing transactions in an SDN network using ZTA+Blockchain technologies

The integration of SDN, Zero Trust, and Blockchain has enabled the development of a multi-phase access request processing algorithm that covers all stages, from initial traffic classification to dynamic security policy enforcement and logging in a distributed registry.

When building an architectural solution, defining the request processing algorithm and laying the foundation for further evaluation of its effectiveness are important. The task is to classify the incoming network traffic as normal or abnormal, which
is the basic scenario for the functioning of Zero Trust and Blockchain audit mechanisms. At the same time, each step of the algorithm must be formalized so that the appropriate evaluation indicators can be applied.

The set of input parameters for the test environment included bandwidth, controller response time, number of sessions and authorization requests, access sources and security policies, and the performance and delays of the Blockchain component. Table 1 describes the input parameters1.

Table 1

Input parameters of the SZB architectural solution

| № | Parameter name | Parameter description |
|---|---|---|
| 1 | Controller throughput | Maximum number of authorisation requests |
| 2 | Maximum controller response time | Time limit for processing a single request |
| 3 | Maximum number of sessions | Total number of sessions for potential re-evaluation |
| 4 | Number of authorisation requests | Total number of requests sent to PDP |
| 5 | Number of access sources | Maximum number of sources undergoing verification |
| 6 | Number of policies in the system | Complete set of security policies in the Policy Repository |
| 7 | Number of sessions in the test | Total number of initiated sessions |
| 8 | Number of re-evaluation requests | All cases of Reeval procedure initiation |
| 9 | Maximum re-evaluation time | Maximum delay for context re-evaluation |
| 10 | Blockchain performance (TPS)) | Maximum number of transactions per second |

| | | |
|---|---|---|
| 11 | Maximum transaction processing time in Blockchain | Maximum number of transactions per second |

Based on the input data, it is necessary to determine whether each request belongs to normal or abnormal traffic. In addition, it is necessary to describe the indicators as a functional system on which the quantitative assessment of SDN network efficiency using ZTA and Blockchain technologies can be based [20].

The proposed algorithm provides comprehensive processing of access requests in SDN, considering the principles of Zero Trust and Blockchain capabilities. Its task is to convert a regular network request into a formalized decision (Permit/Deny) that is transparent, immutable, and subject to quantitative assessment.

At the input, the algorithm receives 'raw' network requests with user attributes and context. The output includes: traffic classification (normal/abnormal), transaction recording in Blockchain, policy adaptation in case of context change, and calculation of performance indicators (CARI, PDPI, BAIS, CAIS), which are aggregated into a generalized iTZBEI indicator. Thus, the proposed algorithm solves both the functional task of dynamic access control and the analytical task of quantitatively assessing the SDN network security level. This task is solved according to the algorithm shown in Fig. 2. Fig. 2 shows the architectural and algorithmic diagram of the SDN architectural solution, reflecting the interaction cycle between the SDN controller, Zero Trust modules, and the Blockchain subsystem. The diagram shows five phases of request processing (SDN initiation, ZTA, Blockchain, solution deployment, re-authorisation), as well as their connection with dimensionless indicators (CARI, PDPI, PSC, STEI, CAIS, BPEI, LPI, RPC, BAIS) that are part of the generalized iTZBEI indicator. Each approved or rejected operation is recorded as a transaction with a digital signature, timestamp, and policy identifiers, forming a reliable audit trail. A step-by-step request processing algorithm was developed to formalize the functioning of the proposed architectural solution, covering five logically complete phases (Fig. 2).

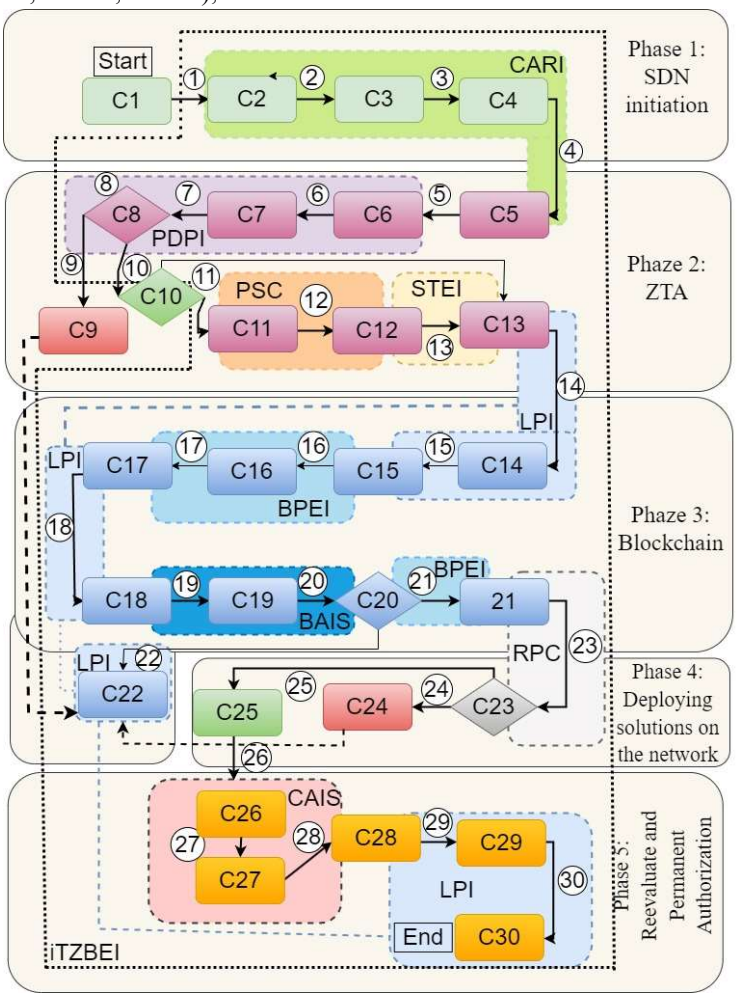


Figure 2. Architectural and algorithmic diagram of the functioning of the SDN + Zero Trust + Blockchain architectural solution with integration of the metrics system

Each phase is responsible for implementing a separate level of security - from initial request processing

at the transport infrastructure level to making access decisions and subsequent audit support for transactions in a distributed ledger.

Table 2 shows the step-by-step processing of a network request in the SDN + Zero Trust + Blockchain architectural solution, reflecting the correspondence between phases, performance indicators, and algorithm blocks (C1–C30).

Table 2

Compliance of SDN + ZTA + Blockchain algorithm steps and performance indicators

| Phase | Step number | Compliance with the Indicator | Compliance with the functional block of the SZB architecture (Fig. 2). | List of actions |
|---|---|---|---|---|
| Phase 1: SDN initiation | 1 | - | C1 | User initiates request |
| | 2 | CARI | C2 | Packet-In to controller - switch response |
| | 3 | | C3 | SDN controller performs initial processing |
| | 4 | | C4 | Controller forwards request to Policy Engine |
| | | | | |
| Phase 2: ZTA | 5 | - | C5 | Controller forwards request to Policy Engine |
| | 6 | PDPI | C6 | PDP receives policy-based request |
| | 7 | | C7 | PDP refers to Policy Inputs |
| | 8 | | C8 | PDP makes a decision |
| | 9 | - | C9 | PDP sends a signal to PE or controller to block access. |
| | 10 | - | C10 | PE receives the decision |
| | 11 | PSC | C11 | PE initiates policy updates (if necessary) |
| | 12 | | C12 | PAP updates the Policy Repository |
| | 13 | STEI | C13 | Formation of session-based flow rules |
| | | | | |
| Phase 3: Blockchain | 14 | LPI | C14 | Request hash is formed |
| | 15 | | C15 | Digital signature is created |
| | 16 | BPEI | C16 | Transaction is formed |
| | 17 | | C17 | Transaction is transferred to Blockchain |
| | 18 | LPI | C18 | Digital signature is verified |
| | 19 | BAIS | C19 | Policies are compared in Blockchain |
| | 20 | | C20 | Smart Contract decision is made |
| | 21 | BPEI | C21 | Return result to controller |
| | 22 | LPI | C22 | Log result in Blockchain |
| | | | | |
| Phase 4: Deployment of solutions across the network | 23 | RPC | C23 | Set access rules (TTL/session) |
| | 24 | - | C24 | Block on Deny |
| | 25 | - | C25 | Grant access on Allow |
| | | | | |
| Phase 5: Reevaluate and ongoing authorisation | 26 | CAIS | C26 | Monitor anomalies |
| | 27 | | C27 | Reevaluate on context change |
| | 28 | | C28 | Repeated PDP decision |
| | 29 | LPI | C29 | Generate repeat transaction |
| | 30 | | C30 | Blockchain records repeat event |

Its ideology is based on combining the logic of architectural components with a system of metrics, which allows the traffic classification process (normal/abnormal) to be formalized and ensures the possibility of quantitative assessment of each step. The step-by-step processing of a request in the SDN + Zero Trust + Blockchain architectural solution and its connection to the metrics system are shown. Each phase of the algorithm is presented as a set of steps, where the corresponding performance indicator and functional block are specified.

Let's consider the phases of solving the following problem:

Phase 1. Initiation and initial analysis of the request (SDN level). A network request arrives at the edge SDN switch, which generates a Packet-In message and forwards it to the SDN controller for centralized verification in accordance with Zero Trust principles. The controller identifies key traffic attributes (IP addresses, ports, protocols) and constructs the request's semantic structure via the Feature Extractor module.

Steps C1–C4 are evaluated using the CARI indicator, which characterizes the response adaptability of the SDN controller.

Phase 2. Contextual authorization based on policies (Zero Trust Engine). The collected data are transferred to the PDP, which assesses request compliance with active security policies using external sources, such as SIEM, PKI, and behavioral profiles. If required, the Policy Administration Point (PAP) updates the policy repository, and the resulting decision is translated into Flow Rules for SDN enforcement. Steps C5–C13 are evaluated using the PDPI, PSC, and STEI indicators.

Phase 3. Cryptographic verification and logging (Blockchain layer). Each authorization transaction is recorded in the Blockchain system. The controller generates a request hash and digital signature; a smart contract verifies policy compliance and returns the result, which is simultaneously stored in a distributed audit log. Steps C14–C22 are evaluated using LPI, BPEI, and BAIS indicators.

Phase 4. Deployment of solutions in the infrastructure. Based on the PDP decision, the controller installs Flow Rules with a limited lifetime on the switches, in line with the Zero Trust principle of minimal trust. Access is granted or blocked at the Policy Enforcement Point (PEP). Steps C23–C25 are evaluated using the RPC indicator.

Phase 5. Periodic verification and reauthorization of the study. A continuous monitoring mechanism analyzes user behavior and traffic patterns during active sessions. Context changes trigger a Reevaluation procedure with a new PDP request; the updated decision is recorded as a separate transaction in the Blockchain. Steps C26–C30 are evaluated using the CAIS indicator.

All stages of the model's operation are interrelated and implemented within a closed request processing cycle. The algorithm is presented as a sequence of operations grouped into phases, with the responsible subsystems (SDN, ZTA, Blockchain) specified to increase the structure's transparency. The comparison of phases, components, and corresponding actions is presented in the table below. To further formalize the mechanism of the integrated architecture, the steps described at the phase analysis level were transformed into a corresponding algorithmic structure. The presented algorithm reflects the step-by-step processing of a network request, considering the functional roles of all key elements of the proposed model, particularly the SDN controller, the Zero Trust subsystem, and the Blockchain registry [21].

This approach ensures model transparency and provides a basis for the formal definition of security measurement points to which the corresponding indicators will be applied. These positions will be aligned with the metrics system and the corresponding integral in the following sections.

## 2.2. Formalized description of decision-making when processing an application in SZB

The use of a formalized description is a necessary prerequisite for building an architectural solution. This approach enables a clear definition of the sequence of steps for processing a network request, establishes logical dependencies between system components, and ensures transparency in the decision-making process. Formalization reduces ambiguity in interpretation, creates a basis for algorithmic implementation, and enables the further use of metrics to quantitatively assess the effectiveness of an architectural solution.

In addition, the formalized description integrates the processing stages with the metrics system, allowing each step of the algorithm to be compared with the corresponding performance indicators. This not only increases the reproducibility and scalability of solutions but also enables the localization of vulnerabilities and further optimization of the SZB model.

Classic access systems based on static rules lose their effectiveness in dynamic network environments because they cannot respond to changing contexts and emerging threats. The proposed architectural solution, which combines SDN, Zero Trust principles, and Blockchain functions, implements adaptive access control focused on the context and the actual state of the network [22].

The key functionalities of the algorithm include:

• automated access decision-making based on the current context;

• dynamic policy adaptation based on monitoring data;

• response to anomalies and threats, with subsequent recording of events in an immutable Blockchain ledger [23].

Thus, the model supports both proactive and reactive modes of operation, ensuring transparency of decisions, evidence-based reasoning, and full traceability of all actions.

The decision-making algorithm is structured in three logically connected stages:

• Request evaluation: The SDN controller analyses the incoming access parameters, and the Policy Decision Point (PDP) analyses the user's behavioural and contextual profile.

• Policy adaptation: When changes or anomalies are detected, the PDP initiates rule updates through the Policy Administration Point (PAP). These changes are applied in real time.

• System response: The Policy Enforcement Point (PEP) implements the accepted measures, and the event is recorded as a transaction in the Blockchain, verified by a smart contract.

In this process, all components - SDN controller, PDP, PAP, smart contracts, event log, monitoring agents - act as a coordinated system, providing context-

*ISSN 1814-4225 (print)*
*ISSN 2663-2012 (online)*

sensitive, evidence-based and adaptive access control.

Let us denote actions in the system as follows:

$R = \{U, Res, Act, T_s, C_{tx}\}$ - access request (set of parameters),
where U - unique user identifier;
Res - resource to which access is requested;
Act - type of operation (e.g., read, write);
$T_s$ - request initiation timestamp;
$C_{tx}$ - set of contextual attributes.

$P_i = \{P_1, P_2, \dots, P_n\} = \langle Cond_i, Dec_i \rangle$ - set of access policies,
where P - universal space of system access policies;
$P_i$ - a separate access policy from the P set; $Cond_i$ - access predicate, i.e. a logical condition that determines under which user or environment parameters the request can be executed;
$Dec_i$ - policy decision made based on the results of the condition check, where:

$[\![Dec_i \in \{Permit, Deny\}$ - policy decision

where, (Permit - allow access, Deny - deny access).

$$Auth(R) = f_{PDP}(R, P) = \begin{cases} Permit, & \text{if } \exists P_i: Cond_i(R) = True \wedge Dec_i = Permit \\ Deny, & \text{otherwise} \end{cases}$$ -
authorization function,

$TX = \langle R, \sigma_u, Decision \rangle$ - transaction with authorisation result,
where R - access request;
$\sigma_u$ - digital signature of user u;
Decision - decision.

$S = \{s_1, s_2, \dots, s_k\}$ - security input signals,
where $S$ - is a formalized representation of all triggers that initiate verification and authorization processes in the integrated model.

$\Delta Ctx$ - detected context change.

$$Reeval(R, Ctx + \Delta Ctx) \rightarrow Auth'(R) \rightarrow \rightarrow NewDecision$$ - re-evaluation procedure,
where $Reeval(\cdot)$ - re-evaluation procedure activated when security conditions or user behavior change;
Ctx - current access context;
$\Delta Ctx$ - context change;
$Ctx + \Delta Ctx$ - updated context that takes into account both the previous state and the new conditions;
$Auth'(R)$ - re-authorisation of the R request based on the new context NewDecision - updated access decision: approval, restriction or block.

$TX' = \langle TX\_ID, u, res, op, T', ctx, P_i' DEC', \sigma_{PEP} \rangle$ - revaluation transaction,
where TX_ID - unique identifier of the revaluation transaction (links it to the initial request or creates a new entry in the log),
u - identifier of the user or agent that initiated access;
res - resource being accessed (e.g., service, virtual machine, network segment);
op - type of operation (read, write, modify, transfer data, etc.);
$T'$ - new timestamp reflecting the moment of re-evaluation of access;
ctx - updated request context (current role, location, device status, behavioral parameters);
$P_i'$ - access policy that was applied at the time of reassessment (may differ from the initial one due to changed conditions);
$DEC'$ - the result of the decision made after reassessment (Permit or Deny);
$\sigma_{PEP}$ - digital signature of the Policy Enforcement Point (PEP) module, which certifies the fact of reassessment and records it in the Blockchain.

The proposed architectural solution's coordinated interaction among SDN, Zero Trust, and Blockchain components ensures continuous security verification, flexible responses to context changes, and the recording of all decisions in a distributed registry. Formalizing both initial and repeated decisions as transactions allows them to remain unchanged and facilitates further auditing [28].

Smart contracts play an active role in this architecture, going beyond simple logging [28]. They:

- automatically verify decisions generated by PDP;
- block the application of incorrect or outdated policies;
- initiate reassessment when repeated anomalies are detected;
- record all actions with timestamps and digital signatures in Blockchain.

Thus, the smart contract acts as an independent arbitrator in the access control process, ensuring the reliability and immutability of all system actions.

## 2.3. Algorithmic representation of the decision-making process and policy adaptation

Figure 3 illustrates the complete decision-making logic of the proposed SZB architecture, which presents a formalized block diagram of the transaction processing algorithm. Unlike conventional flowcharts, the diagram directly integrates mathematical expressions within each processing block, establishing an explicit and rigorous link between the architectural components and the formal descriptions introduced in Section 2.2.

The algorithm operates in the SDN control plane and covers ten logically connected steps. The process begins with request generation $R = \{U, Res, Act, T_s, C_{tx}\}$ and initial PDP authorization $D(t) = \{Dec\_i \mid Cond\_i(R(t)) = True, P\_i \in P\}$ (steps 1–2). The authorization function $Auth(t) = f\_PDP(R(t), P, \theta\_ZTA)$ determines the initial Permit/Deny decision (step 2.1), subject to response time monitoring $T\_resp(t) > T\hat{}max\_resp$ (step 2.2). A positive decision triggers SDN rule formation $FR(t) = \langle MatchFields(R(t)), Actions(u(t)), TTL(t)\rangle$ with TTL calculated as $TTL(t) = min\{TTL\_max, \alpha \times T\_session\}$ (steps 5.1–5.4), followed by Blockchain audit logging $tx\_FR(t) = Verify/Log(E\_FR(t))$ (step 5.5). A negative decision results in access blocking with a corresponding audit transaction $tx\_D(t) = Verify/Log(E\_D(t))$ (steps 3.1–3.4).

For active sessions, the continuous re-evaluation trigger $ReevalTrigger(t) = \{d(C\_tx(t), C\_tx(t + \Delta t)) > \varepsilon\}$ monitors contextual deviations (step 7). When triggered, re-authentication $Auth'(t) = f\_PDP(R(t), P, \theta\_ZTA)$ and rule updating $FR'(t) = \langle MatchFields, Actions, TTL\rangle$ are initiated (steps 8.1–8.2), followed by re-authorization and Blockchain recording of the updated decision (steps 9–9.6). The cycle concludes with a final Blockchain audit $tx\_end(t\_end) = Verify/Log(E\_end(t\_end))$ upon session termination (step 10.1).

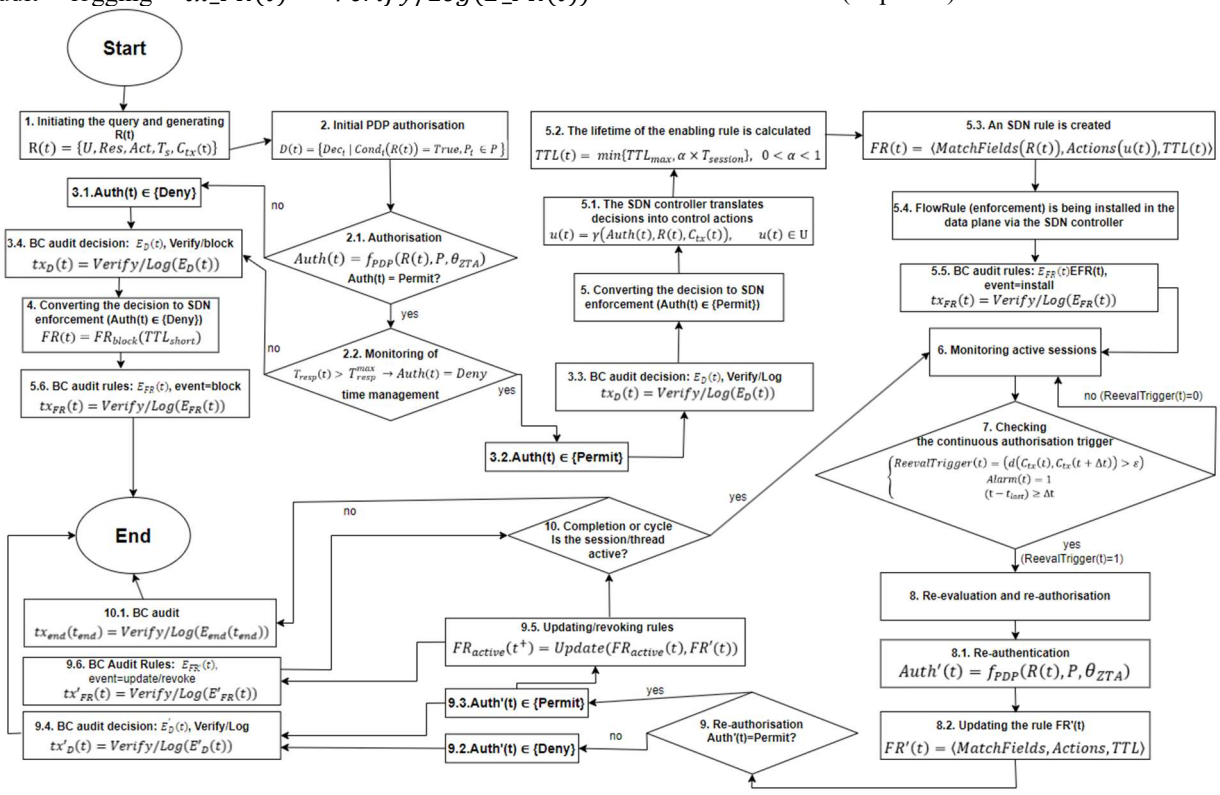


Figure 3. Formalized transaction processing algorithm of the SZB architecture with integrated performance indicators.

Thus, the diagram serves a dual purpose: it demonstrates the operational logic of the integrated architecture and establishes formal measurement points for each processing step, to which the security indicators introduced in Section 4 are directly mapped. The experimental environment used to validate the proposed model under realistic network conditions and attack scenarios is presented in the following section.

## 3. Experimental setup

Simulation testing was performed in a virtualized environment using Mininet for SDN network modeling and Hyperledger Fabric for Blockchain implementation to validate the proposed security model. We recreated interaction scenarios and system responses to potential threats using conditionally generated input data corresponding to realistic network requests and typical attack characteristics. Although the results do not claim exhaustive empirical validation, they provide a quantitative basis for assessing the model's stability, adaptability, and scalability before deployment in more complex environments.

The test network included six hosts, two OpenFlow switches, and one SDN controller. OpenDaylight, configured according to Zero Trust principles, performed centralized flow management and implemented microsegmentation – each host was isolated and could initiate communication only after passing authentication and authorization procedures. Hyperledger Fabric served as a decentralized event log, storing access requests, PDP

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

decisions, authorization results, and digital signatures, with transaction validation and record immutability being ensured by smart contract emulation [25]. All components were deployed on a physical server with an Intel Core i7 processor, 32 GB RAM, and 1 TB SSD running Ubuntu 22.04.

### 3.1. Input parameters and testing environment to obtain metrics

Fig. 4 shows a structural diagram of the integration of Zero Trust principles and Blockchain technology in an SDN environment. It illustrates the interaction of hosts through switches under the centralized control of a controller that implements access policies according to the Zero Trust model.

Each request for a connection between nodes is checked according to defined rules, after which the authorization result is recorded in the Blockchain registry to ensure immutability and traceability of events. Thus, the diagram demonstrates the full access cycle: from the initiation of the request by the host to the update of the distributed event log.

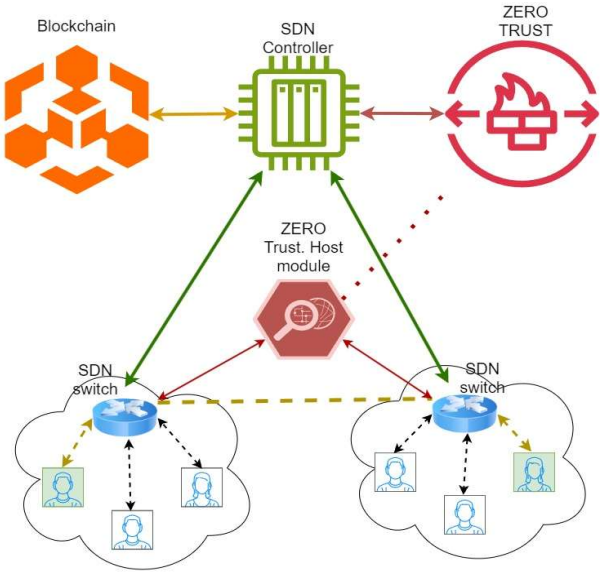


Figure 4. Scheme of the experimental installation of the SZB architectural solution

To recreate the experimental environment and ensure reproducibility of the results, a set of input parameters was defined that characterizes the controller constraints, the behavior of the authorization system, and the performance of the Blockchain component.

Each testing stage covered the interaction of SDN, Zero Trust, and Blockchain components within the full access cycle: from submitting a request to its authorization, recording in the Blockchain, and responding to changes in behavioral parameters. In the test cycle, requests from the host to protected resources were artificially initiated. The OpenDaylight controller performed the initial check, activated microsegmentation rules, and forwarded requests to the PDP module for decision-making in accordance with Zero Trust policies. If necessary, the system launched reevaluation procedures, including context updates and reauthorization.

Traditional metrics, such as latency or throughput, are insufficient for evaluating the multi-layered SZB architecture, which includes access control, trust verification, policy management, and blockchain Logging components. To address this, a system of dimensionless indicators that enables quantitative assessment of both individual functional blocks and the system as a whole is proposed.

Table 3 shows the key parameters used during the integrated model simulation.

Table 3

Test environment input parameters

| № | Parameter name | Value |
|---|---|---|
| 1 | Controller throughput | 500 pcs |
| 2 | Maximum controller response time | 15 ms |
| 3 | Maximum number of sessions | 500 pcs |
| 4 | Number of authorization requests | 190 pcs |
| 5 | Number of access sources | 4 pcs |
| 6 | Number of policies in the system | 85 pcs |
| 7 | Number of sessions in the test | 160 pcs |
| 8 | Number of re-evaluation requests | 60 pcs |
| 9 | Maximum re-evaluation time | 120 ms |
| 10 | Blockchain throughput (TPS) | 13.3 tx/s |
| 11 | Maximum transaction processing time in the Blockchain | 150 ms |

The indicators are grouped into three levels: the SDN+ZTA level, reflecting PDP decision accuracy, controller adaptability, policy stability, and continuous reauthorization quality; the SDN+Blockchain level, characterizing transaction processing performance, log

integrity, and audit reliability; and the universal iTZBEI indicator, which aggregates all local indicators into a single weighted value for holistic security assessment. The proposed metric system provides a scalable and adaptive evaluation framework suitable for comparing alternative configurations and supporting real-time security monitoring.

## 4. Complex of security indicators for the SZB architecture

### 4.1. SDN + Zero Trust Metrics

**CARI (Controller Adaptive Response Index).** The CARI metric evaluates the effectiveness of an SDN controller in handling access requests under Zero Trust conditions, taking into account the response speed and the frequency of re-evaluates. It is defined as a weighted combination of three metrics: successfully processed Packet-Ins, relative authorization latency, and re-evaluation rate. Units of measurement: dimensionless value (from 0 to 1)

Purpose: shows how quickly and efficiently an SDN controller handles Packet-In requests, taking into account delays and re-evaluates.

$$CARI=\omega_1\times\left(\frac{N_{packet\_in}^{handled}}{N_{packet\_in}^{total}}\right)+\omega_2\times\left(1-\frac{T_{avg\_auth}}{T_{max\_auth}}\right)+\omega_3\times\left(1-\frac{N_{reeval}}{N_{flows}}\right) \quad (1)$$

where $N_{packe\ in}^{handled}$ - number of Packet-In requests processed by the controller successfully (pcs.);

$N_{packet_{in}}^{total}$ - total number of received Packet-In requests (pcs.);

$T_{avg\_auth}$ - average authorization time (ms);

$T_{max\_auth}$ - maximum allowable authorization time (ms) defined by the SLA policy;

$N_{reeval}$ - number of re-checks of authorization;

$N_{flows}$ - total number of installed flows (flow rules);

$\omega_1$, $\omega_2$, $\omega_3$ [0;1] - weight coefficients that determine the importance of each indicator in the model (for example: $\omega_1$=0.4, $\omega_2$=0.3, $\omega_3$=0.3).

The CARI indicator is a dimensionless quantity within the interval [0;1], where values close to 1 indicate high efficiency of the SDN controller in the context of processing authorization requests. An increase in the indicator value indicates a decrease in the average response time of the system, a decrease in the load on the decision-making mechanism (PDP), as well as a decrease in the number of repeated authorizations during an active session. The interpretation of the indicator values is given in Table 4:

Table 4

SDN controller performance evaluation using the CARI

| CARI value range | Efficiency level | Interpretation |
|---|---|---|
| 0.0 – 0.3 | Low efficiency | The controller is overloaded, high latency, many reevaluates. |
| 0.3 – 0.7 | Satisfactory performance | The system works stably, but with noticeable delays or checks. |
| 0.7 – 0.9 | High efficiency | The controller responds quickly, most requests are processed with minimal delay. |
| 0.9 – 1.0 | High efficiency | Almost perfect system response. No or insignificant rechecks. |

Thus, the CARI indicator allows for a comprehensive assessment of the performance and stability of the SDN controller's response as a key executive component in the Zero Trust architecture.

**PDPI (Policy Decision Precision Index).** The PDPI evaluates the accuracy of PDP decisions, taking into account how fully the context is used during authorization. It reflects the proportion of decisions made based on extended data. Units: dimensionless value (from 0 to 1)

Purpose: determines how much the system's policy decisions (authorizations) are based on the full context (for example, data from SIEM, behavioral models, PKI, etc.).

$$PDPI=\frac{N_{auth}^{contextual}}{N_{auth}^{total}}\times\frac{S_{input}}{S_{max}} \quad (2)$$

where, $N_{auth}^{contextual}$ - the number of authorizations performed with full context checking (pcs.);

$N_{auth}^{total}$ - the total number of authorizations performed by PDP (pcs.);

$S_{input}$ - the number of Policy Inputs sources actually used when making a decision (pcs.);

$S_{max}$ - the maximum possible number of context sources available in the system (pcs).

Table 5

PDPI Policy Decision Accuracy Rating Scale

| Value range | Accuracy Level | Interpretation |
|---|---|---|
| 0.0 – 0.3 | Low Context | PDP makes decisions without taking into account important sources of Policy Inputs; |
| 0.3 – 0.6 | Limited Context | Some contextual sources are used, decisions are partially justified. |
| 0.6 – 0.85 | Full Context | PDP takes into account most relevant sources, which ensures reliability. |
| 0.85 – 1.0 | Maximum Accuracy | PDP uses all available contexts - decisions have the highest level of trust and accuracy. |

The PDPI indicator, like other indicators, is a dimensionless quantity in the range [0;1], which allows you to assess the level of contextuality of decisions made. The more context is used, the higher the accuracy and validity of political decisions.

The PDPI indicator is key to determining the level

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

of "intelligence" authorization in the system

**PSC (Policy Stability Coefficient).** The PSC measures the stability of access policies in a Zero Trust system by assessing change frequency relative to the current load. Its purpose is to detect excessive dynamism, which may indicate poor administration or external influence. Units of measurement: Dimensionless value (from 0 to 1)

Purpose: Determines the stability of policy settings in the system. It measures how often policies are updated (via PAP) relative to the total pool of valid rules.

$$PSC=1-\frac{N_{pap\_updates}}{N_{policies}^{valid}}\times\frac{1}{1+\lambda} \quad (3)$$

where, $N_{pap\_updates}$- the number of changes initiated by PAP per unit of time (pcs);

$N_{policies}^{valid}$ - the number of active (valid) policies in the repository (pcs);

$\lambda = \frac{N_{auth\_request}}{T_{interval}}$ - the load factor (for example, the average number of authorizations per minute or the level of current requests).

Table 6

PSC Policy Decision Accuracy Rating Scale

| Value Range | Policy stability | Interpretation |
|---|---|---|
| 0.0 – 0.3 | Unstable policy | Policies are constantly updated; false authorization, PAP confusion. |
| 0.3 – 0.6 | Moderate instability | Policies change frequently, but it is a controlled process; the system responds to environmental dynamics. |
| 0.6 – 0.85 | Stable policy | Most policies are long-term, changes are implemented in a reasoned manner through PAP. |
| 0.85 – 1.0 | High stability | Policies change rarely-the system is mature, predictable, and reliable. |

The PSC indicator is also a dimensionless quantity in the range [0;1], which indicates the degree of stability of political rules in the system. Values close to 1 indicate a mature system, where policies are updated only when necessary. Conversely, low values may signal excessive dynamism or failures in governance. The interpretation of the indicator values is given in the table 6:

Overall, PSC is an important factor in determining the maturity of political governance in the Zero Trust model.

**STEI (Session Trust Efficiency Index).** The STEI evaluates the effectiveness of maintaining trust within an active session without excessive re-authentication. This is a key parameter for assessing the balance between security and performance in Zero Trust. Units: dimensionless value (from 0 to 1).

Purpose: shows how effectively the system maintains trust within a single session without unnecessary re-verifications.

$$STEI=\frac{N_{flows}^{session}}{N_{flows}^{total}}\times\left(1-\frac{N_{reeval}}{N_{flows}^{session}}\right) \quad (4)$$

where, $N_{flows}^{session}$ is the number of flows created using session-based flow rules (pcs);

$N_{flows}^{total}$ is the total number of flow rules installed in the system (pcs);

$N_{reeval}$ is the number of re-verifications (Reevaluate) that were initiated for these flows (pcs).

The STEI is also a dimensionless quantity in the range [0;1]. It indicates how effectively the system maintains the level of trust across sessions without unnecessary intervention or checks. The interpretation of the indicator values is given in the table 7:

Table 7

STEI Political Decision Accuracy Rating Scale

| Value Range | Performance Level | Interpretation |
|---|---|---|
| 0.0 – 0.3 | Sessions are unstable or ineffective | Flow rules are frequently re-evaluated, system cannot maintain trust for the duration of the session. |
| 0.3 – 0.6 | Partially effective | Sessions are allowed, but often require re-evaluating; system is unstable. |
| 0.6 – 0.85 | Highly effective | Most sessions do not require re-authorization; flow rules work according to TTL. |
| 0.85 – 1.0 | Maximum session trust | Session-based access is implemented effectively, checks are performed only when necessary. |

This metric is important for balancing authorization automation and responding to changing user or device behavior.

**CAIS (Continuous Authorization Integrity Score).** CAIS characterizes the quality of the continuous authorization mechanism in a Zero Trust environment [26], taking into account the accuracy of detecting deviations and the timeliness of the response.

Units of measurement: dimensionless value (from 0 to 1)

Purpose: assesses the accuracy, relevance and timeliness of re-checks (Reevaluate), which is the main principle of Zero Trust.

$$CAIS=\frac{N_{reeval}^{valid}}{N_{reeval}^{total}}\times\left(1-\frac{T_{reeval}}{T_{session}}\right) \quad (5)$$

where, $N_{reeval}^{valid}$ is the number of re-authorizations that detected valid threats or deviations (pcs.);

$N_{reeval}^{total}$ is the total number of Reevaluates initiated;

$T_{reeval}$ is the average re-check execution time (ms);

$T_{session}$ is the average session duration (ms).

The CAIS indicator is evaluated within the range [0;1]. It determines how accurately and timely the system performs re-authorizations in response to a change in context. The interpretation of the indicator values is given in the table 8:

Table 8

CAIS Political Decision Accuracy Rating Scale

| Value Range | Quality level | Interpretation |
|---|---|---|
| 0.0 – 0.3 | Low revalidation efficiency | The system either over-verifies or does so too late; trust is lost or abused. |
| 0.3 – 0.6 | Moderate efficiency | Re-verifications are sometimes accurate. |
| 0.6 – 0.85 | High authorization accuracy | Most re-verifications are justified and timely; |
| 0.85 – 1.0 | Maximum trust in continuous authorization | Re-authorization is fast, accurate, and contextually informed. |

This Indicator is critical to ensuring the flexibility and sustainability of the Zero Trust model.

### 4.2. SDN + Blockchain Metrics Complex

Integrating Blockchain technology into an SDN environment significantly increases the level of trust in the infrastructure due to the immutability of records, decentralized logging and the ability to independently audit events and policies. This approach enables preserving the history of network solutions, control the integrity of logs and ensure transparency of access to critical resources.

However, the effectiveness of this integration is determined not only by reliability, but also by technical parameters: transaction processing time, failure rate, level of preservation of access rules and the ability to thoroughly verify changes.

**BPEI (Blockchain Processing Efficiency Index)**. The BPEI evaluates the efficiency of transaction processing in the Blockchain component, taking into account the system throughput and the average latency when writing to the registry. It enables quantitative determination of stable the Blockchain infrastructure works in the conditions of integration with SDN. Units of measurement: dimensionless value (from 0 to 1).

Purpose: characterizes how efficiently transactions are processed in a system integrated with Blockchain.

$$BPEI=\frac{TPS_{real}}{TPS_{max}}\times\left(1-\frac{D_{avg}}{D_{max}}\right) \quad (6)$$

where $TPS_{real}$ - actual number of transactions per second;

$TPS_{max}$ - maximum possible number of transactions per second;

$D_{avg}$ - average transaction confirmation latency;

$D_{max}$ - maximum allowable confirmation latency.

A BPEI value close to 1 indicates that the system is operating stably, with high throughput and minimal latency. A value below 0.5 indicates network congestion, processing delays, or inefficient Blockchain infrastructure configuration. The interpretation of the indicator values is given in the table 9:

Table 9

Evaluating the efficiency of transaction processing

| Value Range | Efficiency Level | Interpretation |
|---|---|---|
| 0.0 – 0.4 | Low Efficiency | Blockchain system is not coping with the load: transactions are processed slowly, |
| 0.4 – 0.7 | Satisfactory Performance | The system is functioning, but with periodic delays in transaction confirmation, partially slowed performance. |
| 0.7 – 0.9 | High Efficiency | Blockchain processes transactions quickly, most confirmations are completed with minimal delays, the system scales well. |
| 0.9 – 1.0 | Optimal Performance | The system demonstrates almost perfect processing speed even under heavy load, delays are absent or minimal. |

Thus, the BPEI provides a quantitative assessment of the transaction processing performance of the Blockchain component of the integrated model. Its enables identification of potential bottlenecks in processing requests under high load and serves as a reliable benchmark for comparing the efficiency of different Blockchain infrastructure configurations.

**LPI (Log Provenance Integrity).** LPI characterizes the integrity of the origin of logs in the Blockchain system, determining how reliably and unchangeably the source of each record is recorded. The indicator allows you to assess the transparency of log generation and detects potential attempts at falsification or changes after storage.

$$LPI=\frac{N_{valid\_origin}}{N_{total\_logs}}\times\frac{1}{1+\frac{N_{violations}}{N_{total\_logs}}} \quad (7)$$

where $N_{valid\_origin}$ is the number of logs with a reliably confirmed origin (authenticated source);

$N_{total\_logs}$ is the total number of logs in the system;

$N_{violations}$ is the number of invalid logs;

$N_{total\_logs}$ is the total number of logs that were created or transmitted by the system in the selected time period.

The more reliably confirmed logs and the fewer anomalies, the higher the level of trust in the logging

system. An LPI value close to 1.0 indicates that the Blockchain reliably records provenance, protects integrity, and maintains transparency. A decrease in LPI indicates potential vulnerabilities in logging or an imperfect verification mechanism.

The interpretation of the indicator values is given in the table 10:

Table 10

Assessment of the immutability of log provenance

| Value Range | Integrity Level | Interpretation |
|---|---|---|
| 0.0 – 0.4 | Low | A significant portion of logs have no confirmed origin, possible threats of forgery |
| 0.4 – 0.7 | Moderate | Some logs have authentic origin, but there are anomalies. |
| 0.7 – 0.9 | High | The vast majority of logs are reliable, rare cases of interference. |
| 0.9 – 1.0 | Maximum Trust | All logs have authentic origin, the integrity of the logging system is preserved. |

Thus, the LPI is a critical indicator of trust in event logs in systems with an integrated Blockchain. It allows you to assess the extent to which the system guarantees the immutability of logs and the authenticity of their sources, which is especially important for conducting secure audits, responding to incidents, and verifying past actions. A high LPI value indicates a reliable architecture with a transparent and secure logging mechanism, while a decrease in the Indicator signals potential threats of forgery, unauthorized changes, or insufficient verification of sources.

**RPC (Rule Persistence Coefficient).** RPC reflects the stability of access rules recorded in the Blockchain and allows you to estimate the duration of their validity until they are changed or revoked. This indicator is important for determining the life cycle of policies in a dynamic SDN environment and detecting excessive variability of rules, which may indicate failures or external influences.

$$RPC=\frac{T_{avg\_rule}}{T_{ideal}}\times\frac{1}{1+\frac{N_{updates}}{N_{rules}}} \quad (8)$$

where $T_{avg\_rule}$ is the average lifetime of an established rule (in seconds);

$T_{ideal}$ is the theoretically acceptable average duration of the policies;

$N_{updates}$ is the total number of updates, reinstallations, or overwrites of rules (flow rules) in the system during a specified time interval;

$N_{rules}$ is the number of unique established rules in the same time window.

The interpretation of the indicator values is given in the table 11:

Table 11

Evaluating the stability of rules using the RPC

| Value Range | Strength Level | Interpretation |
|---|---|---|
| 0.0 – 0.4 | Low | Frequent rule changes, short lifetime, possible instability or attack. |
| 0.4 – 0.7 | Moderate | Some rules persist, others are frequently updated; system is unstable. |
| 0.7 – 0.9 | High | Most rules work stably for a given interval. |
| 0.9 – 1.0 | Maximum Strength | Policies remain active for expected time; minimal updates. |

Thus, the RPC Index allows you to assess how consistently the rules are implemented in the system and whether the logic of the long-term effect of approved policies is observed. A high RPC value demonstrates the orderliness, validity and stability of network control, while a low one may signal instability or the need for additional system security verification.

**BAIS (Blockchain Auditability Integrity Score).** BAIS is designed to quantify the quality of auditing in security systems using Blockchain. Despite the immutable nature of Blockchain, the effectiveness of auditing depends on the integrity of the block chain, the accuracy of timestamps, and the availability of records for verification.

The score takes these aspects into account, allowing to determine how suitable the system is for transparent and reliable verification.

$$BAIS=\alpha\times A_{chain}+\beta\times T_{sync}+\gamma\times V_{access} \quad (9)$$

where $A_{chain}$ [0,1] is the degree of chain integrity: reflects the absence of lost blocks, failures, forks, or conflicts;

$T_{sync}$ [0,1] is the accuracy of synchronization of timestamps in blocks;

$V_{access}$ [0,1] is the availability of data for verification;

α,β,γ-weight coefficients that are set depending on the priority (for example: α=0.4,β=0.3,γ=0.3).

The interpretation of the indicator values is given in the table 12:

Table 12

Audit assessment according to the BAIS Indicator

| Value Range | Audit Transparency Level | Interpretation |
|---|---|---|
| 0.0 – 0.4 | Low | The chain is unstable, timestamps are unreliable, auditability is not possible. |
| 0.4 – 0.7 | Moderate | Access to some blocks is limited or there are delays/inconsistencies |

| | | |
|---|---|---|
| | | in synchronization. |
| 0.7 – 0.9 | High | Almost all blocks are available, there are minimal discrepancies in time or structure. |
| 0.9 – 1.0 | Full Transparency | The system is fully auditable: integrity, availability, synchronicity are preserved. |

The BAIS metric acts as an integral indicator of the transparency and integrity of a Blockchain log, allowing for a quantitative determination of whether a system is suitable for full audit. This is especially important for high-liability environments where falsification or loss of logs is unacceptable.

**iTZBEI aggregated indicator**. The iTZBEI indicator is formed based on the aggregation of nine predefined dimensionless indicators, grouped into two main levels - the ZTA component and the Blockchain component. It reflects the degree of consistency between policy decisions, session stability, network performance and data integrity. The indicator is calculated using the formula using weighting factors:

$$iTZBEI=\sum_{i=1}^{9}\omega_i\times I_i=\omega_1\times CARI+\omega_2\times PDPI+\omega_3\times PSC+\omega_4\times \\ \times STEI+\omega_5\times CAIS+\omega_6\times BPEI+\omega_7\times LPI+\omega_8\times RPC+\omega_9\times BAIS \quad (10)$$

where $I_i$ is the normalized value of the corresponding indicator;

$\omega_1$, $\omega_2$, …, $\omega_9$ [0;1] - weighting factors that determine the importance of each indicator in the model.

The iTZBEI aggregated index is a key tool for quantifying the effectiveness of a unified security model based on the interaction of SDN, Zero Trust, and Blockchain. It allows not only to compare different architecture configurations, but also to continuously monitor the security status of the system in real time.

Since the iTZBEI aggregated index (Integrated Trust–ZTA–Blockchain SDN Efficiency Index) is formed as an aggregate value based on local indicators, it is necessary to establish reasonable weighting factors that determine the contribution of each indicator to the final value. This approach allows you to adapt the assessment to the specifics of the environment and ensures control over security priorities at each level. The interpretation of the indicator values is given in the table 13:

Table 13

Interpretation of the meaning of iTZBEI

| Value | System Rating | Interpretation |
|---|---|---|
| 0.0–0.4 | Low Efficiency | Components are working inconsistently, there is a delay or errors in the decision |
| 0.4–0.7 | Moderate Efficiency | The system is working, but there are significant shortcomings in authorization or event storage |
| 0.7–0.9 | High Efficiency | The architecture is working smoothly, most indicators meet the standards |
| 0.9–1.0 | Optimal Performance | Full integration and consistency of components, rapid response and protection |

The weighting coefficients $\omega_1 - \omega_9$ are determined through a structured expert assessment procedure based on three evaluation criteria: functional significance of each component within the SZB architecture, frequency of its involvement in the operational cycle, and vulnerability criticality - the sensitivity of the component to attacks or failures affecting overall system resilience. For each indicator $\omega_i$, expert scores $ss_i^{(1)}, s_i^{(2)}, s_i^{(3)}$ are assigned on a scale of 1–5, after which an integrated importance score is computed as:

$$q_i = \beta_1 s_i^{(1)} + \beta_2 s_i^{(2)} + \beta_3 s_i^{(3)} \quad (11)$$

where $\beta_1 + \beta_2 + \beta_3 = 1$.

The normalized weight for each indicator is then derived as:

$$\omega_i = \frac{q_i}{\sum_{k=1}^{9} q_k} \quad (12)$$

where $\omega\_i \in [0,1]$ and $\sum_{k=1}^{9} q_k$, ensuring a normalized aggregated index within the range [0;1].

The baseline weight distribution used for reproducible comparisons is presented in Table 14.

Table 14

Example of weighting factors

| Indicator | Index | Value | Explanation |
|---|---|---|---|
| $\omega_1$ | CARI | 0.15 | Packet-In processing speed is critical |
| $\omega_2$ | PDPI | 0.10 | Accuracy of PDP policy decisions |
| $\omega_3$ | PSC | 0.10 | Stability of PAP policies |
| $\omega_4$ | STEI | 0.10 | Reliability of session authorization |
| $\omega_5$ | CAIS | 0.10 | Quality of continuous authorization review |
| $\omega_6$ | BPEI | 0.15 | Blockchain process performance |
| $\omega_7$ | LPI | 0.10 | Log integrity |
| $\omega_8$ | RPC | 0.10 | Network rule life cycle |
| $\omega_9$ | BAIS | 0.10 | System auditability |

CARI and BPEI are assigned the highest weights (ω = 0.15) reflecting the elevated importance of SDN controller responsiveness and Blockchain transaction efficiency, while the remaining indicators maintain a balanced contribution (ω = 0.10). Where required, the weights may be adapted to the target deployment domain - corporate networks, IoT segments, or critical infrastructure - provided the normalization constraint $\sum\omega\_i = 1$ is preserved across all configuration variants.

The proposed indicator system is designed not merely as a performance measurement tool, but as a security-oriented evaluation framework in which each metric directly reflects a specific vulnerability or threat vector identified in Section 1. The mapping between security properties and indicators operates at two levels.

At the ZTA layer, five indicators address the core security challenges of dynamic access control. CARI quantifies the resilience of the SDN controller to request overload, serving as a direct measure of resistance to DDoS attacks on the control plane – a degraded CARI value signals that the controller is approaching a state exploitable by volumetric attacks. PDPI measures the contextual completeness of PDP decisions, reflecting the system's ability to prevent unauthorized access through policy bypass or credential misuse, low PDPI indicates decisions made without sufficient contextual verification, increasing the risk of false authorization. PSC detects excessive instability in the policy repository, which may indicate external manipulation of access rules or insider interference with the PAP, abnormal PSC fluctuations serve as an early warning signal for policy-level attacks. STEI evaluates the effectiveness of session-level trust maintenance, directly limiting the attack surface within active connections by ensuring that compromised sessions are identified and re-evaluated promptly. CAIS assesses the timeliness and accuracy of the Reevaluation mechanism, the primary defense against insider threats and behavioral anomalies, where a low CAIS value indicates that the system is either over-verifying legitimate users or failing to detect genuine deviations in time.

At the Blockchain layer, four indicators address the integrity and auditability of security decisions. BPEI ensures that audit transactions are processed without delay, maintaining the continuity of the security audit chain under high load — degraded BPEI may indicate a Blockchain bottleneck that creates gaps in the audit trail. LPI directly measures the immutability and authenticity of log records, providing a quantitative detection signal for log forgery attempts or unauthorized post-storage modifications. RPC reflects the stability of access rules against unauthorized modification or premature revocation, detecting attempts to manipulate routing rules recorded in the distributed ledger. BAIS quantifies the overall auditability of the system, ensuring that all security events remain independently verifiable — a critical property for forensic investigation and compliance verification.

The iTZBEI index aggregates these nine security-oriented indicators into a single weighted value, providing a holistic and continuous measure of how effectively the integrated SZB architecture protects against the four principal attack categories identified in Section 1: DDoS attacks, control plane compromise, data plane interception, and insider threats.

## 5. Results and Discussion

A test environment based on Mininet with an OpenDaylight controller and a private Hyperledger Fabric Blockchain network was deployed to verify the effectiveness of the proposed model. The testing covered normal operating conditions and scenarios with simulated attacks (particularly DDoS, interference with access policies, and attempts to bypass authorization). During the experiment, key input parameters were recorded, and the corresponding Performance

Indicators covering the performance of SDN components, correct authorizations, logging reliability, and resilience to failures in the Blockchain subsystem were calculated.

The performance of the SZB provided in table 15:

Table 15

Data for calculating the integral indicator iTZBEI

| Index | Value $I_i$ | Coef. $\omega_i$ | Initial data | Normalized value |
|---|---|---|---|---|
| CARI | 0.697 | 0.15 | 460/500 processes, 12ms out of 15, 15 re-evaluates out of 500 | 0.1380 |
| PDPI | 0.80 | 0.10 | 152/190 authorizations, 4/4 sources | 0.0800 |
| PSC | 0.750 | 0.10 | 6 changes out of 85 policies, $\lambda = 0.8$ | 0.0750 |
| STEI | 0.850 | 0.10 | Session flows: 136 out of 160, Reeval: 12 | 0.850 |
| CAIS | 0.600 | 0.10 | 36/60 successful re-evaluates, 18ms out of 120ms | 0.0600 |
| BPEI | 0.880 | 0.15 | 11.76 TPS out of 13.3, 85ms out of 150ms | 0.0900 |
| LPI | 0.900 | 0.10 | Successful hashes: 97 out of 107, Violations: 5 | 0.0900 |
| RPC | 0.950 | 0.10 | Average TTL: 90 sec, Failures: 2 out of 180 | 0.0950 |
| BAIS | 0.700 | 0.10 | Successfully verified: 125 out of 178, $\alpha = 0.5$, $\beta = 0.3$, $\gamma = 0.2$ | 0.0700 |

The calculation:

$$\text{iTZBEI} = 0.1380 + 0.0800 + 0.0750 + 0.0850 + 0.0600 + 0.1320 + 0.0900 + 0.0950 + 0.0700 = \mathbf{0.835}$$

Figure 6 shows a diagram that displays the actual contribution of each local indicator to the overall integral iTZBEI indicator through the product of its normalized value and the corresponding weight coefficient. The two least effective Indicators (CAIS and BAIS) are highlighted in red as potential areas for improvement.

The final value of the iTZBEI indicator = 0.835 corresponds to a high level of efficiency according to the

interpretation scale, which indicates the coordinated operation of the model components in conditions close to the real environment.

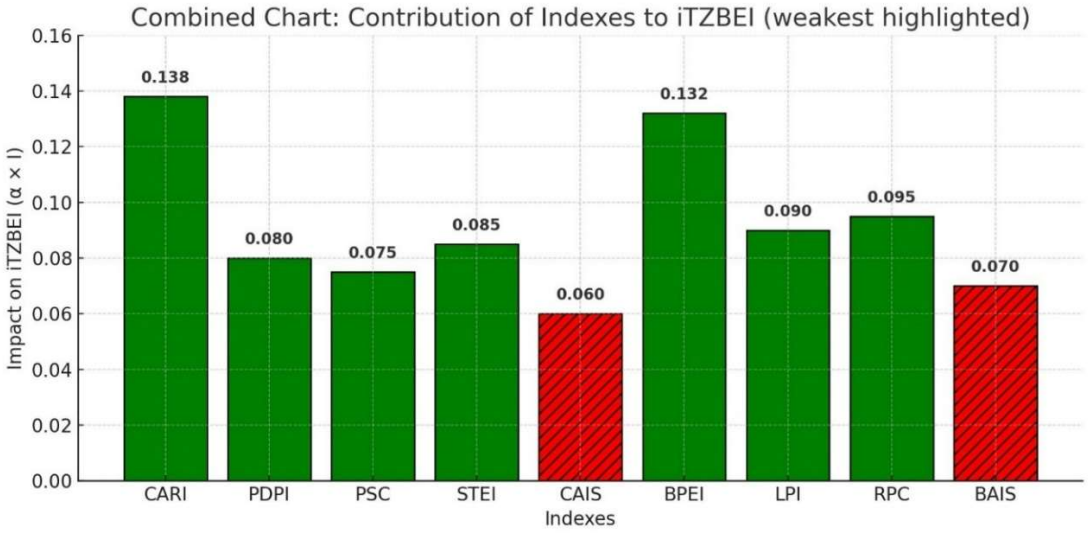


Figure 4. Combo chart: contribution of indicators to iTZBEI

The greatest contribution to iTZBEI was provided by:

• CARI (0.138) - the efficiency of SDN controller adaptation;

BPEI (0.132) - the performance of transaction processing in Blockchain.

In contrast, the CAIS (0.060) and BAIS (0.070) indicators revealed relatively low efficiency. This indicates the need for further improvement of re-authorization mechanisms in the ZTA environment and increased audit transparency in the Blockchain component.

The integral indicator calculation allows not only for quantitative assessment of the overall level of security but also for identification of critical areas of the system. The proposed iTZBEI model can serve as a tool for dynamic monitoring and decision-making in environments with heightened security requirements, owing to its clear metric structure and consistent weighting factors.

### 6. Conclusion and future work

This paper introduces iTZBEI - a composite, dimensionless metric for quantitative security assessment of integrated SDN–ZTA–Blockchain architectures. The proposed system of nine local indicators covers key aspects of each architectural layer, including controller adaptability, authorization policy accuracy, continuous re-verification efficiency, access rule stability, and event log integrity. Experimental validation on a Mininet–OpenDaylight–Hyperledger Fabric environment yielded iTZBEI = 0.835, confirming high overall effectiveness of the integrated architecture while identifying continuous authorization (CAIS) and audit transparency (BAIS) as primary areas for improvement.

The iTZBEI metric provides a scalable and adaptive evaluation framework that enables comparative assessment of alternative configurations, real-time security monitoring, and informed decision-making regarding system configuration in dynamic network environments.

In further research, it is planned to conduct in-depth testing of the proposed model under active cyberattack scenarios – including DDoS attacks on the SDN controller, control and data plane compromises, smart contract vulnerabilities, and insider threats - with the aim of refining the iTZBEI weighting coefficients for deployment in real-world high-threat environments.

**Contributions of authors**: review and analysis of literature – **Oleksandr Pidpalyi, Anton Romanov, Anton Marinov, Nesterenko Mykola**; formulation of the purpose and tasks – **Oleksandr Pidpalyi, Oleksandr Romanov**; development of conceptual provisions and research methodology – **Oleksandr Pidpalyi**; development of mathematical models and methods – **Oleksandr Pidpalyi**; selection and application of software and hardware for modeling and presentation of results – **Oleksandr Pidpalyi, Anton Romanov, Anton Marinov , Nesterenko Mykola**; analysis of research results – **Oleksandr Pidpalyi, Oleksandr Romanov, Larisa Globa**; writing – preparation of the original project – **Oleksandr Pidpalyi**; preparation of materials for publication **Oleksandr Pidpalyi, Anton Romanov, Anton Marinov, Nesterenko Mykola**; writing – review and editing – **Larisa Globa, Oleksandr Romanov.**

All authors have read and approved the final manuscript for publication.

## Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship, or otherwise, that could affect the research and its results presented in this paper.

## Financing

This study was conducted without financial support.

## Data Availability

The manuscript contains no associated data

## Use of Artificial Intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, as described in the research methodology section.

## References

1. Pidpalyi, O. Optimising service quality and network efficiency in legacy networks by integrating SDN and broadband. *Information Technology and Computer Engineering*, 2024, no. 1, pp. 29–42. DOI: 10.63341/vitce/3.2024.29.

2. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. A review and comparative analysis of relevant approaches of Zero Trust Network Model. *Sensors*, 2024, vol. 24, no. 4, article no. 1328. DOI: 10.3390/s24041328.

3. Bassfar, Z., Sayeed, A., Bala, P., Alshehri, A., Alanazi, A. M., & Zubair, S. Toward secure and resilient networks: a Zero-Trust security framework with quantum fingerprinting for devices accessing network. *Mathematics*, 2023, vol. 11, no. 12, article no. 2653. DOI: 10.3390/math11122653.

4. Ma, Y.-W., & Chiu, P.-H. A novel risk-based access control engine in Zero Trust Architecture for IoT network. *International Journal of Information Security*, 2025, vol. 24, article no. 124. DOI: 10.1007/s10207-025-01030-2.

5. Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. Zero-Trust access control mechanism based on Blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, 2025, vol. 25, no. 2, article no. 550. DOI: 10.3390/s25020550.

6. Bhatt, H., Rana, S., & Dubey, S. S. Blockchain-driven decentralized data and access control services for smart grid. *Cluster Computing*, 2025, vol. 28, article no. 755. DOI: 10.1007/s10586-025-05347-4.

7. Hussain, A., Li, S., Hussain, T., Attar, R. W., Alhomoud, A., Alsagri, R., & Alzubi, A. A. Blockchain-enabled Zero Trust-based Secure and Energy Efficient scheme for 6G-enabled UASNs. *Journal of Cloud Computing*, 2025, vol. 14, article no. 21. DOI: 10.1186/s13677-025-00744-x.

8. Alevizos, L., Ta, V. T., & Eiza, M. H. Augmenting Zero Trust Architecture to Endpoints Using Blockchain: a state-of-the-art review. *arXiv preprint*, arXiv:2104.00460, 2021. DOI: 10.48550/arXiv.2104.00460.

9. Li, W., Meng, W., Liu, Z., & Au, M.-H. Towards blockchain-based software-defined networking: security challenges and solutions. *IEICE Transactions on Information and Systems*, 2020, vol. E103.D, no. 2, pp. 196–203. DOI: 10.1587/transinf.2019INI0002.

10. Guo, X., Wang, C., Cao, L., Jiang, Y., & Yan, Y. A novel security mechanism for software defined network based on Blockchain. *Computer Science and Information Systems*, 2022, vol. 19, no. 2, pp. 523–545. DOI: 10.2298/CSIS210222001G.

11. Romanov, O., Nesterenko, M., Boggia, G., & Striccoli, D. Construction and methods for solving problems at the SDN control level. *Lecture Notes in Electrical Engineering*, Cham: Springer, 2023, vol. 965, pp. 77–90. DOI: 10.1007/978-3-031-24963-1_6.

12. Romanov, O., Siemens, E., Nesterenko, M., & Mankivskyi, V. Mathematical description of control problems in SDN networks. *Proceedings of International Conference on Applied Innovation in IT*, 2021, vol. 9, no. 1, pp. 33–39. DOI: 10.25673/36582.

13. Meng, W., Li, W., & Zhou, J. Enhancing the security of blockchain-based software defined networking through trust-based traffic fusion and filtration. *Information Fusion*, 2021, vol. 70, pp. 60–71. DOI: 10.1016/j.inffus.2020.12.006.

14. Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R. M., & Li, G. Automation and orchestration of Zero Trust Architecture: potential solutions and challenges. *Machine Intelligence Research*, 2024, vol. 21, pp. 294–317. DOI: 10.1007/s11633-023-1456-2.

15. Dhar, S., & Bose, I. Securing IoT devices using Zero Trust and Blockchain. *Journal of Organizational Computing and Electronic Commerce*, 2021, vol. 31, no. 4, pp. 18–34. DOI: 10.1080/10919392.2020.1831870.

16. Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., & Shabaz, M. Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications. *Computer Communications*, 2023, vol. 206, pp. 140–152. DOI: 10.1016/j.comcom.2023.04.022.

17. Li, J., Lv, H., Lei, B., & Xie, Y. A consensus approach for SDN controllers based on Blockchain. *CSSE 2022: Proceedings of the 2022 5th International Conference on Computer Science and Software Engineering*, Guilin, China, October 21–23, 2022, pp. 170–174. DOI: 10.1145/3569966.3570015.

18. Wadhwa, S., Rani, S., Kavita, Verma, S., Shafi, J., & Wozniak, M. Energy efficient consensus approach of Blockchain for IoT networks with edge computing. *Sensors*, 2022, vol. 22, no. 10, article no. 3733. DOI: 10.3390/s22103733.

19. Pidpalyi, O., & Romanov, O. Integration of Zero Trust and Blockchain in SDN networks: an overview of threats and methods of their elimination. *Information*

*Technology and Computer Engineering*, 2025, no. 1, pp. 55–68. DOI: 10.63341/vitce/1.2025.55.

20. Li, M., Cheng, H., Cao, W., Yu, S., & Song, J. Access control method of SDN network based on Zero Trust. *Proceedings of ICATCI 2022, Lecture Notes on Data Engineering and Communications Technologies*, 2023, vol. 170, pp. 496–504. DOI: 10.1007/978-3-031-29097-8_59.

21. Gai, K., She, Y., Zhu, L., & Choo, K. K. R. Blockchain-based access control scheme for Zero Trust cross-organizational data sharing. *ACM Transactions on Internet Technology*, 2023, vol. 23, no. 3, article no. 38, pp. 1–25. DOI: 10.1145/3511899.

22. Bicer, C., Murturi, I., Donta, P. K., & Dustdar, S. Blockchain-based Zero Trust on the edge. *arXiv preprint*, arXiv:2311.16744, 2023, pp. 1–9. DOI: 10.48550/arXiv.2311.16744.

23. Iyer, S. Comprehensive smart contract security using a Zero-Trust approach. *ResearchGate preprint*, 2024, pp. 1–20. DOI: 10.13140/RG.2.2.13950.60480.

24. Ma, Z., Chen, X., Sun, T., Wang, X., Wu, Y. C., & Zhou, M. Blockchain-based Zero-Trust supply chain with DRL for inventory optimization. *Future Internet*, 2024, vol. 16, no. 5, article no. 163. DOI: 10.3390/fi16050163.

25. Wijesekara, P. A. D. S. N., & Gunawardena, S. A review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. *Network*, 2023, vol. 3, no. 3, pp. 343–421. DOI: 10.3390/network3030017.

26. Joumaa, H., Petrovska, A., Hariri, A., Dimitrakos, T., & Crispo, B. Continuous authorization architecture for dynamic trust evaluation. *Trust Management XIV, IFIPTM 2023, IFIP Advances in Information and Communication Technology*, Cham: Springer, 2024, vol. 694, pp. 1–18. DOI: 10.1007/978-3-031-76714-2_1.

*Received 18.09.2025, Received in revised form 10.03.2026*
*Accepted date 27.07.2026, Published date 31.07.2026*

## iTZBEI: ІНТЕГРАЛЬНА МЕТРИКА БЕЗПЕКИ ДЛЯ SDN-АРХІТЕКТУР З ІНТЕГРАЦІЄЮ ZERO TRUST ТА BLOCKCHAIN

***О.І. Підпалий, О.І. Романов, Л.С.Глоба, М.О.Романова, М.М. Нестеренко***

***Предметом вивчення в статті є*** *iTZBEI (Integrated Trust–ZTA–Blockchain SDN Efficiency Index) - новий комплексний показник для кількісної оцінки безпеки програмно-конфігурованих мереж (SDN) з інтеграцією концепції Zero Trust Architecture (ZTA) та технологій Blockchain.* ***Актуальність дослідження зумовлена тим, що*** *централізована модель керування SDN генерує критичні вразливості - зокрема DDoS-атаки, несанкціоноване маніпулювання маршрутизацією та внутрішні загрози - для яких наразі не існує єдиної системи кількісного оцінювання.* ***Метою статті є*** *розробка формалізованого агрегованого показника безпеки, що забезпечує безперервний моніторинг та порівняльне оцінювання всіх компонентів архітектури SDN–ZTA–Blockchain.* ***Завдання:*** *(1) ідентифікація основних векторів атак на SDN; (2) формалізація алгоритму обробки транзакцій, що охоплює повний життєвий цикл доступу; (3) визначення дев'яти локальних показників безпеки; (4) побудова індексу iTZBEI з обґрунтованими ваговими коефіцієнтами.* ***Методи дослідження*** *поєднують математичну формалізацію процесів контролю доступу, криптографічну верифікацію транзакцій та експериментальну емуляцію сценаріїв атак у середовищі Mininet–OpenDaylight–Hyperledger Fabric.* ***Отримані результати статті.*** *Розроблено функціональний алгоритм, який виконує динамічну верифікацію запитів користувачів, ухвалює адаптивні рішення щодо авторизації відповідно до принципу мінімальних привілеїв та фіксує ці рішення в незмінному розподіленому реєстрі. Запропоновано систему метрик, що включає локальні показники: Continuous Authorisation Integrity Score (CAIS), Blockchain Audit Integrity Score (BAIS) та Local Policy Integrity (LPI). На цій основі сформульовано інтегральний індекс iTZBEI як агрегований показник для порівняльного оцінювання та безперервного моніторингу стану безпеки мережі.* ***Наукова новизна.*** *У статті запропоновано єдину архітектурну основу SDN+ZTA+Blockchain для забезпечення мережевої безпеки, формалізовано алгоритм обробки транзакцій, що безпосередньо пов'язує рішення про доступ із процедурами розподіленого аудиту, а також введено метрику iTZBEI як перший інтегральний показник для оцінювання ефективності такої інтеграції в динамічних мережевих середовищах.*

**Ключові слова:** ***безпека SDN, Zero Trust, Blockchain, метрики безпеки, цілісність авторизації, iTZBEI, системи аудиту***

**Підпалий Олександр Іванович** – аспірант кафедри телекомунікаційних систем, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна;

**Романов Олександр Іванович** – д-р техн. наук., проф., професор кафедри телекомунікацій, Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна;

**Глоба Лариса Сергіївна** - д-р техн. наук., проф., професор кафедри телекомунікацій, Національний

технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна;

**Романов Антон Олександрович -** аспірант кафедри телекомунікацій, Національний університет «Київський авіаційний інститут», Київ, Україна;

**Марінов Антон Ігорович -** аспірант кафедри телекомунікаційних систем, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна;

**Нестеренко Микола Миколайович -** д-р техн. наук., доцент кафедри комунікаційних систем, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна;

**Oleksandr Pidpalyi –** PhD student, Assistant at the Department of Telecommunication Systems, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
e-mail: sashapidpalyi@gmail.com , ORCID: 0009-0007-6852-7959

**Oleksandr Romanov –** Doctor of Technical Sciences, Professor, Professor at the Department of Telecommunications, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
e-mail: a_i_romanov@ukr.net, ORCID: 0000-0002-8683-3286

**Larysa Globa**- Doctor of Technical Sciences, Professor, Professor at the Department of Telecommunications, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
e-mail: lgloba@its.kpi.ua, ORCID: 0000-0003-3231-3012

**Anton Romanov** - PhD student, National University «Kyiv Aviation Institute», Liubomyra Huzara ave. 1, 03058, Kyiv, Ukraine
e-mail: anton3329@gmail.com ORCID: 0000-0002-3425-0441

**Anton Marinov -** PhD student, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
e-mail: marinov.anton99@gmail.com, ORCID: 0000-0001-8717-2734

**Mykola Nesterenko** – Doctor of Technical Sciences, Associate Professor, Head of the Department of Communication Systems, Military Institute of Telecommunications and Informatization named after Heroes of Kruty, Kyiv, Ukraine.
e-mail: mykola.nesterenko@viti.edu.ua, ORCID: 0000-0003-0812-2793