Architecture of the software system of confidential access to information resources of computer networks*

Yuliia Kostiuk[1,†], Svitlana Rzaieva[1,†], Karyna Khorolska[1,†], Nataliia Mazur[1,†] and Nataliia Korshun[1,*,†]

[1] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract

The paper presents a formalized model of the architecture of a software system that provides confidential access to the information resources of computer networks amid the high dynamism of network infrastructures, the increasing complexity of the information environment, and the heightened requirements for protecting user privacy. The proposed architecture is grounded in the concepts of modularity, openness, and unified software interfaces, which together ensure compatibility with heterogeneous deployment environments. The functional subsystems integrate multi-level authentication, cryptographic encryption, attribute-based access control, anomaly detection in user behavior, and active access monitoring based on artificial-intelligence mechanisms. A mathematical model for assessing the degree of confidentiality of access has been developed, enabling quantification of the security level of information objects in accordance with Zero Trust Architecture standards. The practical significance lies in the architecture's applicability to information systems with stringent confidentiality demands while meeting institutional and regulatory oversight requirements.

Keywords

confidential access, system architecture, information security, computer networks, access control, encryption, multi-level security

1. Introduction

The growing number of cybersecurity incidents accompanying the digital transformation of enterprises requires new approaches to organizing secure access to the information resources of computer networks. Traditional solutions based on centralized access control or classical cryptographic schemes are insufficiently effective in distributed, multi-service environments, where the volume, speed, and variability of traffic demand dynamic, flexible, and adaptive protection.

Of particular importance are software-based confidential-access systems that can provide not only authenticated and authorized access but also preserve the confidentiality of user requests, their sessions, and the history of interactions with network resources. In modern implementations, such systems should support a multi-level security policy, automated access control, distributed architecture, standardized encryption protocols, and interaction with other components of the information infrastructure—including SIEM, VPN, and Zero-Trust environments. These systems must offer open, unified interfaces; a flexible, modular architecture; and the capability to integrate with SIEM, DLP, and VPN solutions, audit tools, digital-identity systems, and secure-transmission protocols (TLS, IPsec, WireGuard, etc.).

The purpose of this paper is to develop an architecture for a software system that enables confidential access to the information resources of computer networks, integrates security mechanisms with artificial-intelligence tools, supports information-security standards, and allows access policies to adapt to the evolving risk landscape of IT infrastructures. The study proposes a

* CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine

* Corresponding author.

† These authors contributed equally.

y.kostiuk@kubg.edu.ua (Y. Kostyuk); s.rzaieva@kubg.edu.ua (S. Rzaieva); k.khorolska@kubg.edu.ua (K. Khorolska); n.mazur@kubg.edu.ua (N. Mazur); n.korshun@kubg.edu.ua (N. Korshun)

0000-0001-5423-0985 (Y. Kostyuk); 0000-0002-7589-2045 (S. Rzaieva); 0000-0003-3270-4494 (K. Khorolska); 0000-0001-7671-8287 (N. Mazur); 0000-0003-2908-970X (N. Korshun)

system model, a mathematical apparatus for assessing the level of confidentiality, and principles for building an open architecture that accommodates third-party software components.

2. Literature review

The issue of designing the architecture of software systems that enable confidential access to information resources is a key topic in contemporary cybersecurity research, where special attention is devoted to adaptive risk-management mechanisms, data protection, and dynamic access control. Althar et al. [1] present an automated risk-management model focused on identifying and eliminating software vulnerabilities. The proposed solution integrates risk-assessment mechanisms directly into the secure-software development process, which is particularly relevant for confidential-access architectures, where resistance to known and potential threats must be ensured from the design stage.

Wang, Ahmad, and Bakar [2] conducted a systematic review of approaches to digital transformation and risk management in small and medium-sized enterprises. The authors emphasize the need to implement flexible and adaptive access-control systems in highly uncertain environments. This conclusion aligns with modern requirements for confidential-access architectures, which must deliver not only security but also scalability and adaptability.

The study by Barraza de la Paz et al. [3] offers a systematic review of risk-management methodologies in complex Industry 4.0 and 5.0 organizations. In particular, the authors highlight the importance of building intelligent information systems capable of self-organization, monitoring user behavior, and analyzing threats in real time. This perspective directly corresponds to the requirements of modern confidential-access software systems deployed in hybrid-cloud environments and infrastructures with distributed access control.

The review by Ahmad et al. [4] addresses security issues in software-defined networks (SDN). The authors analyze key vulnerabilities in centralized network-management models and propose dynamic routing and distributed authentication concepts that can be incorporated into confidential-access system architectures. Given SDN's capabilities for traffic control and the flexible definition of security policies, such approaches can underpin the construction of confidential network segments that isolate critical resources.

Thus, contemporary scientific literature confirms the relevance of creating architectures that support flexible interaction among security components, adaptive access control, and the confidentiality of information processing—factors that collectively form the foundation for developing effective software systems for confidential access in computer networks. Recent research by Vakhula et al. [5] explores the implementation of policy-as-code frameworks for role-based and attribute-based access control, emphasizing automation and precision in managing confidential access rights within complex network environments. Similarly, Susukailo and Lakh [6] propose an innovative access control system leveraging encryption within QR-Code technology, which enhances secure and user-friendly authentication methods suitable for confidential information resource management.

3. Research methods

The research methods are grounded in the theory of algorithmic computational complexity, the reliability of automated control systems, modern cryptographic primitives, distributed programming, and the theory of multi-layer architectures. Additionally, risk-based modelling in accordance with ISO/IEC 27005 and NIST SP 800-30, together with machine-learning techniques for adaptive query analysis, were employed. Formal models of confidential access, fuzzy-logic methods, Bayesian updating, and agent-based interaction within a distributed environment are applied. The combined use of state-of-the-art cryptographic protocols (TLS 1.3, IPsec, SSH-2), Zero-Trust concepts, and integration with SIEM and MFA systems provide an adaptive, scalable architecture for confidential access to critical information resources.

4. Main material

Modern software tools for protecting electronic information can be classified into the following groups: cryptographic protection tools, access-control systems, tools enabling confidential access to information resources, and security mechanisms deployed in financial, educational, and cloud platforms [1, 2]. Analysis and comparison of such systems are necessary to create a unified software-system architecture capable of ensuring both robust data protection and user privacy within the digital environment.

In this context, particular attention is devoted to data-protection solutions based on the IPsec protocol, which provides confidential and authenticated exchanges in TCP/IP networks. Modern mechanisms for building Virtual Private Networks (VPNs) are also examined; they allow secure data exchange between distributed information systems while minimizing infrastructure costs and simultaneously broadening the geographical reach of access [7, 8]. Notable effective implementations include IPsec VPN, SSL VPN, and tunnelling with WireGuard.

Figure 1 illustrates the deployment of the components of a software-based confidential-access system designed in accordance with Zero Trust security principles and contemporary authorization and encryption standards. The architecture comprises a client device, authorization and access servers, a cryptographic gateway, a security-information and event-management (SIEM) system, and cloud services hosting educational, financial, and other resources. The inter-component connections demonstrate the flow of access requests, authorization decisions, cryptographic protections, event logging, and configuration policies. The system supports scalability, adaptability, and integration with external platforms through unified interfaces.

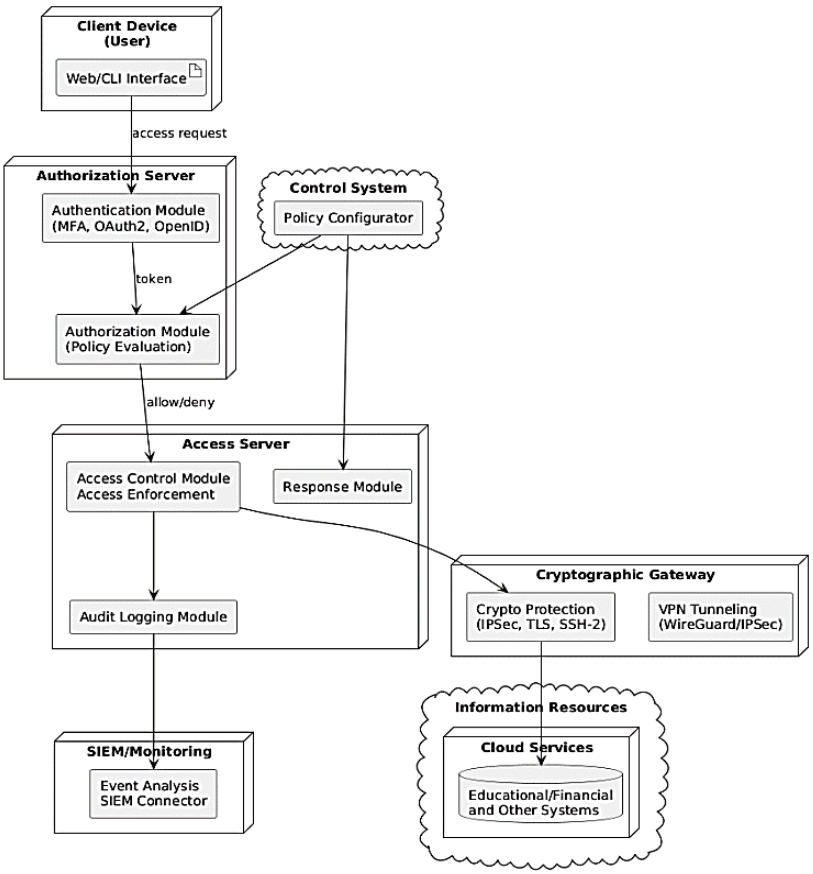

Figure 1: Structure of the generalized architecture of the software system of confidential access to information resources of computer networks

Current multifactor authentication and authorization systems (e.g., OAuth 2.0, SAML, OpenID Connect) are integrated with confidential-access platforms to implement Zero-Trust approaches, in

which no trust is granted to any user or device by default [9]. Microsoft Windows systems employ the Security Support Provider Interface (SSPI) for local authentication, and Linux uses PAM (Pluggable Authentication Modules), which provides flexible management of credentials at the OS-kernel level.

Typical architectures of such systems are characterized by modularity, where the key components are: a module for collecting and analyzing event information, a decision-making module based on security policies, a response module that implements blocking or allowing access, a logging module that records the actions of access subjects for auditing, and a management module that supports dynamic policy configuration in line with environmental changes [10, 11]. An important element is integration with monitoring systems (e.g., SIEM) and the use of next-generation cryptographic protocols—TLS 1.3, SSH-2, and IPsec with Perfect Forward Secrecy (PFS) [4, 12–14].

The component architecture of the software system for confidential access to the information resources of computer networks (Figure 2) is built with due regard for modern data-protection requirements. It includes modules for multifactor authentication, policy-based authorization, and access control in accordance with the Zero-Trust concept. The system features cryptographic protection (IPsec, TLS, SSH-2, WireGuard), event logging, incident response, and monitoring components through integration with SIEM platforms. Access to cloud resources—including educational and financial services—is provided through secure confidential tunnels. The architecture supports dynamic access-rights management, end-to-end encryption, user identification, and traffic protection in accordance with industry information-security standards.

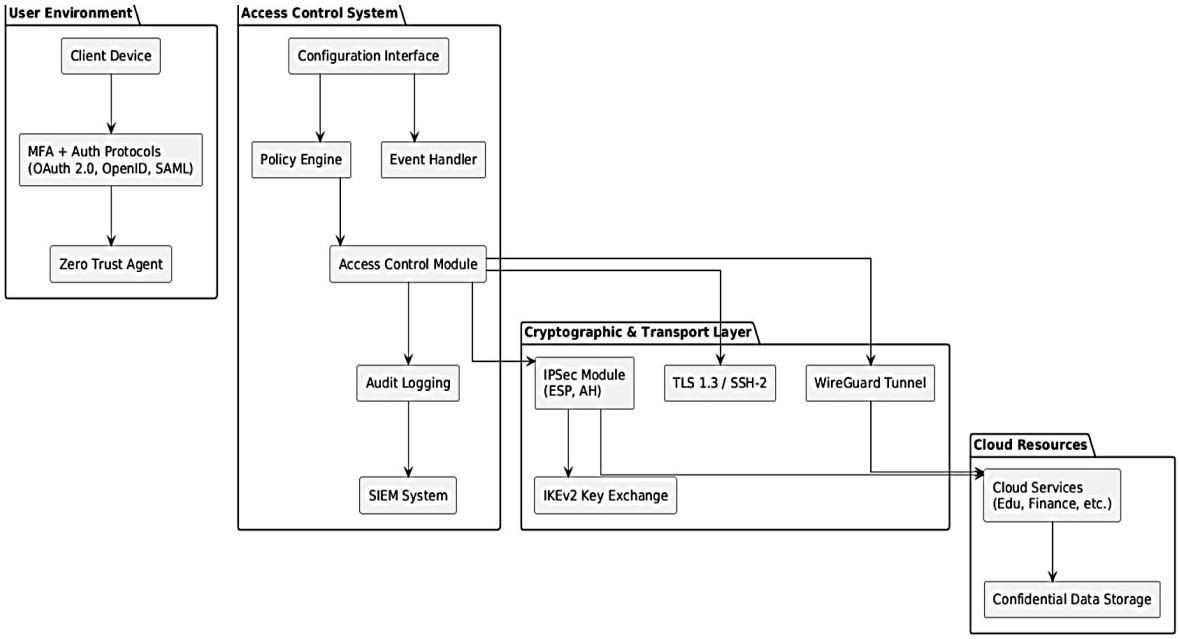

Figure 2: Component architecture of a confidential access system using IPSec

Special attention is devoted to the construction of confidential communication channels. Their organization includes key exchange via the IKEv2 protocol, the use of Encapsulating Security Payload (ESP) for traffic encryption, and Authentication Header (AH) for source verification [4, 8, 15]. Together, these elements form end-to-end encryption and ensure the integrity of transmitted data. Thus, the architecture of a confidential-access software system must meet the following requirements: support for dynamic access control, scalability, compatibility with open protocols, integration with cloud platforms, transparency of access without compromising security, and preservation of the confidentiality of both data and user requests.

The study examines algorithms and architectures for confidential access to information resources, in particular technologies of anonymous virtual networks such as DC-net, Mix-net,

Crowds, Onion Routing, and Freedom Network [16]. These systems implement traffic-protection mechanisms, route obfuscation, and multi-level encryption, which make it impossible to track the source of requests. Particular attention is paid to anonymous networks that are compatible with the application layer of the TCP/IP stack, scalable, and capable of formally assessing the degree of anonymity achieved using mathematical models such as entropy or differential anonymity. The Mix-net architecture, whereby data are transmitted through mix servers that randomly route and reorder messages to reduce the likelihood of correlating requests with responses, is also investigated. Modern software-based confidential-access systems combine these approaches with IPsec VPN, WireGuard, and the Zero Trust concept, in which no device or user is granted a priori trust [11, 17].

The generalized architecture of such systems includes modules for authentication, authorization, response, logging, access-policy management, and traffic encryption using modern cryptographic protocols (TLS 1.3, SSH-2, IPsec with PFS) [8, 12, 13, 15, 18, 19]. Interaction among components is effected through unified interfaces, with integration into SIEM systems for monitoring security events [14, 20]. This configuration enables the creation of a single dynamic software-security framework that supports confidential access to cloud, financial, educational, and corporate resources.

The architecture of the anonymous Mix-net network was reviewed to deepen understanding of the principles underlying confidential-access channels in distributed information environments [16]. This approach facilitated the evaluation of practical mechanisms for protecting traffic at the transport and network layers, including delayed routing, message shuffling, and multi-level encryption. Analysis of the Mix-net architecture proposed by D. Chaum provided a foundation for developing our own dynamic confidential-access system that accounts for anonymity, scalability, and interaction with open TCP/IP protocols. The Mix-net system employs specialized mix servers to transform incoming traffic, altering its sequence and encrypting data at each stage, thereby significantly complicating the correlation between user requests and server responses.

The practical value of this analysis lies in adapting the anonymization principles implemented in Mix-net to the architecture of the system under development, which delivers confidential access to information resources [16, 17, 21]. This adaptation enabled the inclusion of a route-obfuscation module, the establishment of end-to-end encryption, and the assurance of privacy without compromising functionality. Consequently, the study of the Mix-net architecture has supplied tools and conceptual approaches that are integrated into a holistic software-security architecture to enhance request anonymity, implement Zero Trust principles, and establish secure routes to critical network resources.

The diagram (Figure 3) depicts the complete sequence for routing an anonymous user request to a secure resource over the Mix-net network, incorporating Java Anonymizer Proxy (JAP) as the initial proxy service. In the first stage—Anonymous Request Routing—the user submits a request through JAP, which applies the first layer of encryption. The request then proceeds to Mix Server 1, where it is re-encrypted (Layer 2), is forwarded to Mix Server 2 for another encryption layer (Layer 3), and finally reaches Mix Server 3, which performs final processing and relays the request to a secure resource, such as a financial, cloud, or educational system. The second stage—Response Routing—traces the return path from the resource back to the user: the response travels through Mix Server 3, where it is again encrypted, passes through Mix Server 2 and Mix Server 1 with corresponding re-encryption layers, and is ultimately received and decrypted by JAP for the user. The diagram illustrates the full cycle of request and response processing within a secure environment that adheres to principles of end-to-end encryption, route obfuscation, multi-layer encryption, and source-anonymity protection. The combination of these approaches in a single scenario demonstrates the practical implementation of a confidential-access architecture that not only safeguards traffic at every stage but also effectively counters correlation attacks and traffic analysis, thereby maintaining the privacy and integrity of information exchange in computer networks.

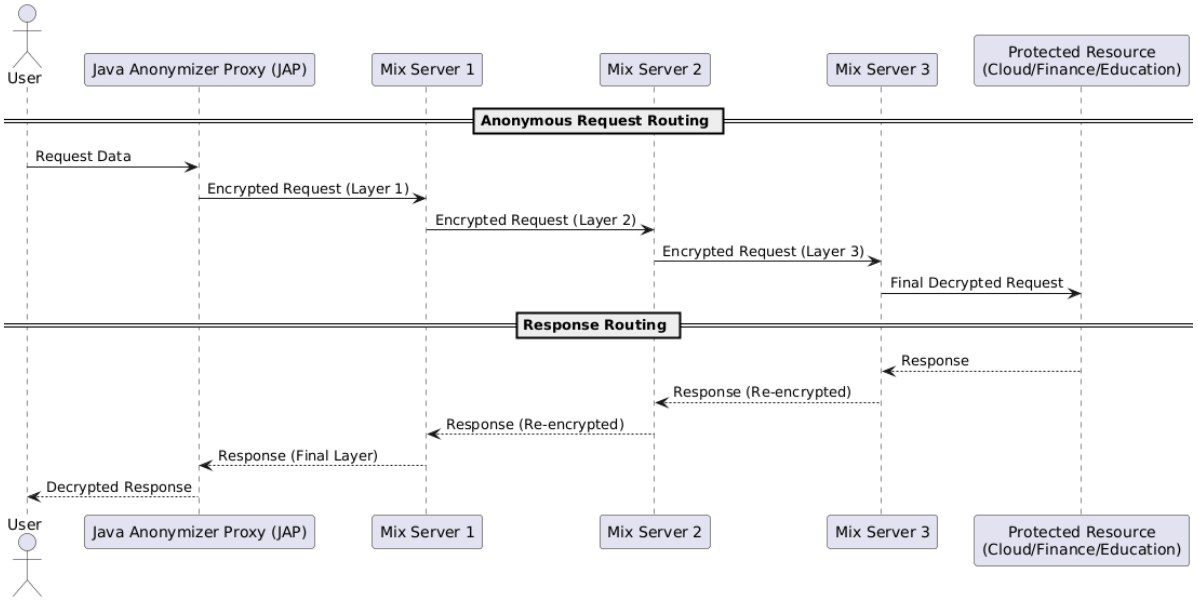

Figure 3: UML diagram of the sequence of an anonymous request and response over the Mix-net network using the JAP proxy

The study proposes a formalized mathematical model and appropriate methods for implementing confidential access in computer networks, focused on the protection of critical information resources [1–3, 15, 21, 22]. The result of an information system vulnerability analysis is a quantitative assessment of its information security level, which can be represented as a function of time during which data is guaranteed to remain confidential, integral and accessible. All requests are controlled by a security infrastructure that includes a security policy controller [10, 11, 20]. The model is easily scalable to any number of segments without losing generality.

The information system is modeled as a set of objects:

$$O = \{o_1, o_2, \dots, o_n\}, \tag{1}$$

where each o_i is an information resource that stores or processes data. Set O represents all objects of the information system, which can be either stored data or components that process information (e.g., databases, services, files).

Entities interacting with the system:

$$S = \{s_1, s_2, \dots, s_n\}, \tag{2}$$

where each s_j—user, device, or software agent. Set S describes the subjects of the information system, i.e. everyone who can access objects: users, devices, processes, agents.

Each object and subject is assigned a security rank from a partially ordered set:

$$R = \{r_1, r_2, \dots, r_n\}, \text{ where } r_0 < r_1 < \dots < r_k, \tag{3}$$

Set R—are security ranks that are ordered by the degree of trust. They are used to categorize both subjects and objects by level of sensitivity or trust. For example: r_0—public information, r_k—the highest level of confidentiality.

As for the access control policy model, the access ranking function is used:

$$g: S \times O \longrightarrow R, \tag{4}$$

Function $g(s, o)$ defines the level of security required for an entity s to gain access to an object o. This mapping is used to determine the minimum subject rank required to access the corresponding object in the system. In other words, it reflects the minimum rank that a subject must have in order to access an information resource.

Maximum access level of the subject:

$$rang(s) = \{g(s, o) \vee\ o \in O\}, \tag{5}$$

Determines the highest level of access that subject s has among all the objects that he or she can access. This allows the system to determine the general level of privileges of this user.

Minimum level for an external attacker:

$$rang\left(s_{\text{attacker}}\right) = \{R\} = r_0, \tag{6}$$

For an external attacker, the lowest possible access level is set to $-r_0$, which means no trust. This is the starting point for analyzing potential threats.

The access decision is formalized as a binary function:

$$Access(s, o) = \{1, \text{if } rang(s) \geq rang(o)\, 0, otherwise, \tag{7}$$

where $rang(s) = \{g(s, o) \vee\ o \in O\}$, a $g: S \times O \longrightarrow R$ is a ranking function. It is a binary decision-making function for granting access. If the security level of the subject is not lower than the security level of the object, access is allowed (1), otherwise—is denied (0).

The model for assessing the level of confidentiality over time is based on the exponential decrease in the probability of maintaining data confidentiality:

$$C(t) = P_{secure}(t) = e^{-\lambda t}, \tag{8}$$

where λ is the intensity of the risk or attack, and t is the time of data retention. The model reflects that over time, the probability that information will remain confidential without additional protection measures decreases exponentially. The presented function is an important tool for formalized analysis of the loss of confidentiality in dynamic information systems. Thus, the proposed model allows us to mathematically describe privacy dynamics, adapt access policies to the time characteristics of data storage, and increase the efficiency of confidential access architectures in computer networks.

To build a more flexible protection system, the concept of a multilevel security model is introduced, in which each component of the IT system is assigned a specific protection level [3, 4, 10]. This model enables the differentiation of access levels, the definition of security policies, the formalization of privilege-granting principles, and the detection of violations based on a comparison of the ranks of subjects and objects. The system supports the implementation of these methods within the confidential-access architecture, which comprises modules for authentication, authorization, encryption, monitoring, and auditing [11, 20, 23]. Consequently, the presented mathematical model formalizes the processes of assessing information security and confidentiality, ensuring the adaptive construction of access policies and their dynamic adjustment in response to environmental changes [1, 3, 21]. This capability is fundamental to the deployment of contemporary software architectures for secure access to computer networks.

The diagram (Figure 4) illustrates the logic of the software system that provides confidential access to the information resources of computer networks. The system performs access control by comparing the security ranks of subjects and objects, which are determined during the ranking process. Access requests are processed in accordance with established policies that incorporate security parameters and current threat models. Decisions to grant or deny access are logged and analyzed by the SIEM system to detect anomalies or unauthorized actions originating from either legitimate users or potential attackers. The diagram depicts the interaction among the user, access controllers, policies, data objects, and monitoring systems.

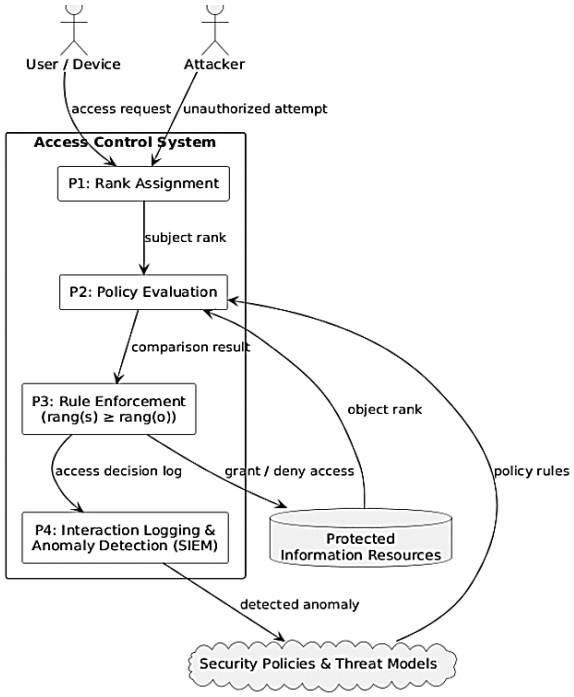

Figure 4: Formalized access control system based on security ranking

The concept of a multi-level information-security model for automated data-processing systems involves structuring system components according to their protection level and functional purpose. This model enables clear delineation of areas of responsibility, minimizes the risk of compromise, and supports the application of adaptive security policies at different logical tiers. In particular, Level A encompasses users' internal client devices; Level B protects an isolated information resource (for example, a web application that processes confidential data); Level C comprises the network infrastructure that supports internal interaction; and Level D represents external users and the channels through which they access the system via public networks—most notably, the Internet [17, 21, 23]. Such stratification facilitates flexible access control, well-reasoned security zoning, and effective identification of potential attack vectors within each level.

Within the confidential-access model, all system principals are divided into the following logical groups: session initiators—users or devices that request resources; relay servers—nodes that obfuscate traffic routes (e.g., Mix servers or Tor nodes) [16]; receiving servers—components that process user requests; information storage—a distributed database that holds anonymized data; and third-party resources—services outside the architecture with which data are exchanged.

In the proposed architecture of the confidential-access software system, data are transferred in accordance with cryptographic-protection principles, ensuring confidentiality, integrity, and authenticity at every stage of the route. Repeaters (intermediate nodes that relay encrypted packets between the client and the target server) employ symmetric-encryption keys, enabling rapid processing of large traffic volumes with minimal latency [24]. Symmetric encryption is effective for tunnelling information when keys are pre-shared or transmitted over a secure channel. Receiving servers (route endpoints) use asymmetric cryptography—specifically, public-key mechanisms—which allows them to accept session keys or user requests securely without a pre-established shared secret [13]. This approach guarantees secure connection establishment even with previously unknown clients. Users (request initiators) generate session-access keys, which are derived using a cryptographic function:

$$K_{session} = F(x, k), \tag{9}$$

where x is the random variable (nonce or initialization vector) that ensures the uniqueness of each connection, k is the encryption key, which can be symmetric or obtained by exchanging

through asymmetric methods (for example, through ECDH), $F(x,k)$ is the cryptographic key calculation function (e.g., HMAC, PBKDF2, or HKDF) [1]. Thus, data confidentiality is ensured through multi-level encryption, where each stage from the user to the target resource implements the appropriate cryptographic mechanisms [8, 24–26]. This approach allows not only to preserve the privacy of the transmitted data but also to ensure resistance to man-in-the-middle (MitM) attacks, session replay, and correlation analysis of traffic.

To build an anonymous channel, a route model in the form of a sequence of nodes is used:

$$\gamma = \langle s_1, s_2, \dots, s_n, g \rangle, \tag{10}$$

where s_i are relay servers, g is the target receiving server [24, 27].

The probability that user u was the source of the request through the confidential communication system (CCS), in the absence of a priori information, is defined as:

$$P(R) = \frac{1}{|PS|}, \tag{11}$$

where PS is the set of potential sources of the request. If the intruder has information about the node through which the traffic passed, the set of possible routes decreases. In the case of building a route without repetitions (without cycles), the number of possible options is calculated as a combination of:

$$C_{b-1}^{j} = \frac{(b-1)!}{j!(b-1-j)!}, \tag{12}$$

where b is the number of available repeaters, j is the length of the route. If the use of repetitions (loops) is allowed, then the number of possible route options is defined as:

$$N = (b-1)^{j}, \tag{13}$$

These mathematical models allow for a formalized assessment of the level of user anonymity and the probability of channel compromise. The functional blocks of the system implement: access control based on policies and the Zero Trust model [17, 23], route obfuscation through multi-stage encryption, cryptographic traffic protection (TLS 1.3, IPsec, WireGuard) [8, 11, 21, 25], audit and monitoring with support for SIEM systems, and dynamic adaptation of security policies [14]. Thus, the proposed confidential access architecture allows implementing anonymous data transmission routes, following the principles of trust minimization and mathematical security verification. It is scalable, integrates with cloud and enterprise environments, and provides flexible access control in complex threat environments.

In a situation where an attacker captures the first node of the route (or another part of the request transmission path), he can partially exclude certain nodes from the set of potential request sources, thereby reducing the degree of user anonymity. In this case, a model with filtering is used to calculate the updated conditional probability that user u initiated the request:

$$P(b,j,m,k) = \frac{1}{|PS| - |NS|}, \tag{14}$$

where $|PS|$ is the initial number of possible sources (potential users), $|NS|$ is the number of excluded (known or compromised) route nodes, b is the route length, j, m, k are route selection parameters (e.g., depth, bypass strategies, number of mixes). The formula reflects the decrease in anonymity: the more nodes an attacker can exclude (i.e. $|NS|$ increases), the higher the probability of correctly identifying the source of the request [14, 16, 20, 27]. Thus, the model allows us to quantify the loss of anonymity under the influence of partial route compromise, which is important for assessing the resistance of a confidential access system to correlation attacks.

Total probability of identity disclosure for a given route:

$$P(b)=\sum_{k=0}^{b} P(b,j,m,k), \tag{15}$$

In the case of an arbitrary access route length in a confidential communication system (CCS), when all valid lengths have the same probability (uniform distribution), the total probability that user uuu was the source of the request is calculated by the formula:

$$P(b)=\frac{1}{b_{\max}-b_{\min}+1}\sum_{j=b_{\min}}^{b_{\max}}\sum_{k=0}^{j} P(j,m,k), \tag{16}$$

where $b_{\min}$ and $b_{\max}$ are minimum and maximum route length, j is the specific route length, k is the route parameter, such as the number of known nodes or the level of filtering, $P(j,m,k)$ is the conditional probability with fixed route parameters. The model takes into account the variability of the data transmission route in a secure system and allows you to assess the degree of user anonymity. The uniform distribution of lengths means that all possible routing scenarios are considered equally likely, which is a typical assumption in systems such as Mix-net or Tor [16]. At the same time, an evidence-based approach is used to assess the cryptographic security of a confidential access system. It is based on modeling cryptographic functions as a family of mappings $F:\{0,1\}^{*}\times\{0,1\}^{*}\longrightarrow\{0,1\}^{*}$, where the first argument is the input data, and the second is the encryption key. The attacker A is represented as a probabilistic Turing machine with time and number of calls to the function. Its attack capability is estimated by the difference between the probability of successfully guessing the result when working with real function F and random function U:

$$adv(F)=|P(A^{F}=1)-P(A^{U}=1)|, \tag{17}$$

where A^{F} is the attacker who has access to the function F, A^{U} is the same attacker, but with access to a random (ideal) generator U, $P(\cdot)$ is the probability of a successful attack [8, 13]. This indicator determines the degree of difference between the function F from a random the point of view of an attacker. The closer this value is to zero, the more secure the cryptographic function and the entire system is considered to be. Thus, the combination of route anonymity and provable cryptographic strength forms a comprehensive security assessment in modern CCS. The closer $adv(F)$ to zero, the more reliable the function F is in terms of cryptanalytic protection.

The level of reliability of the cryptographic function F under the given conditions is defined as:

$$insec_{F}(t,q)=adv(F), \tag{18}$$

where $A(t,q)$ is the set of possible attacks that have no more than t computational steps and q requests. The formalized value indicates the highest probability of successful hacking of the function F under conditions of limited attacker resources. The lower the value of $insec_{F}$, the higher the cryptographic strength of the function in a particular environment.

In the context of a cryptographic protocol $E:K\times R\times P\longrightarrow C$,describing a probabilistic encryption scheme, the security of the system against a Chosen Plaintext Attack (CPA) is evaluated using the expression [13]:

$$adv_{\mathrm{CPA}}(E)=|P(A^{E_k}=1)-P(A^{U}=1)|, \tag{19}$$

where A is the attack algorithm (attacker), E_k is the encryption with a secret key k, U is the random function (the standard of complete unpredictability). The indicator reflects the difference between the probability that an attacker will successfully distinguish encryption with a real algorithm from a random function. The lower the value adv_{CPA}, the more resistant the system is to

CPA attacks, meaning that an attacker cannot effectively distinguish between ciphertexts, even if he can choose plaintexts.

Accordingly, a system is considered CPA-resistant if:

$$insec_{\mathrm{CPA}}^{E}(t,q,l)=adv_{\mathrm{CPA}}(E)<\epsilon, \tag{20}$$

where ϵ is an acceptable level of cryptographic resistance. This formalized approach provides a basis for building a software system that guarantees a high level of confidential access and can adapt to modern information security requirements in computer networks. It combines theoretical principles with practical cryptographic tools, allowing the implementation of attack-resistant architectures with support for dynamic access policy, SIEM integration [14], Zero Trust model [17, 23], and a multi-level resource hierarchy.

To extend the formalized approach to building a software architecture for confidential access in computer networks, mathematical models are used that take into account time dynamics, multi-level trust, adaptability of access policies, and attack resistance. They are truly integrated with Zero Trust mechanisms and analytical capabilities of SIEM systems, creating a flexible and secure information processing platform. Dynamic privacy assurance feature:

$$A_{conf}(s,o,t)=\alpha\cdot Access(s,o)\cdot e^{-\lambda t}, \tag{21}$$

The formula estimates the level of confidential access of a subject s to an object o at the moment of time t, where α is the weighting factor of the resource's criticality, λ is the threat intensity, $Access(s,o)$ is the access permission (1 or 0). The exponential decay reflects the loss of trust in the resource over time.

Effective level of access of an entity:

$$R_{eff}(s)=\sum_{o\in O}\delta(s,o)\cdot g(s,o), \tag{22}$$

where $\delta(s,o)=1$, if access is allowed, and 0 otherwise, $g(s,o)$ is the access rank. The formula summarizes the subject's access levels to all allowed objects, determining the subject's real influence in the system.

Privacy loss rate:

$$\tau_{\mathrm{policy}}(t)=\frac{dC(t)}{dt}=-\lambda\cdot e^{-\lambda t}, \tag{23}$$

The rate of privacy loss $\tau_{\mathrm{policy}}(t)$ shows how quickly the probability of maintaining data confidentiality decreases over time. This indicator is used to dynamically adjust access policies in accordance with the rate of information security loss.

Probability of anomaly detection [14]:

$$P_{\mathrm{anomaly}}(u,t)=1-e^{-\beta\cdot f(u,t)}, \tag{24}$$

where $f(u,t)$ is the user behavior function u, β is the sensitivity of the SIEM algorithm. This model takes into account changes in behavior to predict potential threats. Probability of anomaly detection $P_{\mathrm{anomaly}}(u,t)$ assesses how likely the system is to detect suspicious user behavior u at the time t, taking into account the intensity of deviations $f(u,t)$ and sensitivity of the SIEM mechanism β.

Assessment of user confidence [14, 20]:

$$Q_{trust}(s)=\omega_1\cdot Auth(s)+\omega_2\cdot Hist(s)+\omega_3\cdot SIEM(s), \tag{25}$$

Assessment of user confidence $Q_{\text{trust}}(s)$ is a formalized indicator that allows to quantify the level of trust to the subject s in the system. It combines three main components: the result of authentication $Auth(s)$, behavioral access history $Hist(s)$ nd signals received from the SIEM monitoring system $SIEM(s)$. Each component has its own weight ω_i, that reflects its importance in the overall assessment. This model allows for adaptive decision-making to allow or restrict access, especially in environments that use Zero Trust principles.

Privacy gradient in parameter space:

$$D_{\text{adj}}(p,t)=\nabla_p C(p,t), \tag{26}$$

Privacy gradient in the parameter space $D_{\text{adj}}(p,t)$ reflects how the level of confidentiality C of a resource changes at a certain point in time t depending on its characteristics. This indicator allows you to determine in which direction you need to change access or security parameters to ensure a stable level of confidentiality. It is a useful tool for dynamically adjusting security policies, especially in a changing environment or at increased risk.

System resistance to crypto attacks [9, 26]:

$$\zeta_{\text{resilience}}=\min\left\{insec_F(t,q), insec^{E}_{\text{CPA}}(t,q,l)\right\}, \tag{27}$$

The system's resistance to cryptoattacks $\zeta_{\text{resilience}}$ determines the worst-case security scenario by comparing the vulnerability to general probabilistic attacks $insec_F(t,q)$ and chosen plaintext attacks (CPA) $insec^{E}_{\text{CPA}}(t,q,l)$. The minimum value among them is selected, which indicates the least resistant component. The lower this indicator is, the higher the cryptographic reliability of the system as a whole. It allows you to formally evaluate the effectiveness of encryption algorithms and justify their suitability for use in a secure access architecture.

Average effective privilege:

$$\Phi_{\text{access}}=\frac{1}{n}\sum_{i=1}^{n} Access(s_i,o_i)\cdot r(o_i), \tag{28}$$

Average effective privilege Φ_{access} allows you to quantify the overall level of access in the system, taking into account both the fact of access granted and the sensitivity of each object $r(o_i)$. The formula calculates the average value of privileges for all active access sessions, where each contribution is weighted according to the level of confidentiality of the resource. A high value of the indicator may indicate the risk of excessive access to sensitive objects, which requires increased control.

Privacy entropy is a formalized metric that allows to assess the uniformity of privacy distribution among information objects in a computer network. It is determined using the Shannon formula:

$$H_{conf}=-\sum_{i} P(o_i)\cdot \log_2 P(o_i), \tag{29}$$

where $P(o_i)$ is the probability that an object contains or processes confidential information. This indicator allows you to quantify how well the confidential resources are distributed within the network. If the entropy is high, this indicates an even distribution of confidentiality, when no single object concentrates a significant amount of critical information. On the other hand, a low entropy value means that there are objects with an excessive concentration of confidential data, and these objects are critically vulnerable to attacks or information leaks. This situation requires an immediate review of security policies in order to redistribute the load, strengthen control, or isolate the most risky objects. Thus, the privacy entropy indicator plays an important role in making decisions on adaptive risk management, developing security zones, and determining priority areas

for the application of cryptographic protection and monitoring [10, 23]. It is an integral element of a formalized approach to building a flexible, dynamic and stable architecture of a software system for confidential access to information resources of computer networks. The Zero Trust policy application index, defined as:

$$\Lambda_{\text{zero}_{\text{trust}}}(u) = 1 - Q_{\text{trust}}(u) \cdot P_{\text{anomaly}}(u, t), \tag{30}$$

formalizes the principle of dynamic management of user trust u in systems based on the Zero Trust model [17, 21, 23]. In this model, trust is not granted to any user or device by default, and each request is verified in the context of current behavior, action history, and analytical monitoring results. The value of $Q_{\text{trust}}(u)$ reflects the level of accumulated trust in the subject based on multifactor authentication, analysis of past user behavior, access history, and SIEM system responses [14, 20]. At the same time $P_{\text{anomaly}}(u, t)$ simulates the probability of detecting anomalous user actions at a certain point in time t, calculated on the basis of behavioral patterns and risk profiles [20]. Index $\Lambda_{\text{zero}_{\text{trust}}}(u)$ actually describes the degree to which restrictive measures should be applied to the user. The lower the trust in the user and the higher the likelihood of anomalies, the higher the index value, meaning that the system should act more cautiously, restricting or blocking access, introducing additional layers of verification (for example, additional MFA or contextual confirmation). In the case of $Q_{\text{trust}}(u) \to 1, P_{\text{anomaly}}(u, t) \to 0$, value of $\Lambda_{\text{zero}_{\text{trust}}}(u) \to 1$, indicating that there is no need for additional control, as the user demonstrates stable, trusted behavior.

Thus, the formula allows to implement an adaptive security policy that automatically adjusts according to the current user behavior and trust assessment, which is a key element in the implementation of a modern architecture of confidential access to computer networks [17, 20, 21, 23]. Thanks to this mechanism, the system becomes capable not only of responding to incidents but also of proactively preventing threats by forming a real-time access policy taking into account many risk factors, which significantly increases the overall level of information security.

According to contemporary digital-security requirements, the architecture of a software system for confidential access to the information resources of computer networks must provide flexibility, scalability, and resistance to a wide range of attacks [1, 12, 24]. The central element of this architecture is a modular platform built on secure network protocols, modern cryptographic algorithms, and adaptive access-control mechanisms. The system comprises the following components: an administrative console, information probes (event sensors), security controllers, SIEM components for centralized event analysis, secure entry points with multi-factor authentication, traffic repeaters for tunnelling requests through isolated zones, and modules for processing requests to the information-storage subsystem [13, 17, 21, 23]. All of these elements interact through secure channels based on TLS 1.3, IPsec, or WireGuard, with support for Perfect Forward Secrecy.

The administrative console enables administrators to manage access policies, configure modules, and monitor incidents in real time. It communicates with other system components—including security controllers, SIEM modules, entry points, and traffic repeaters—to ensure operational management and rapid incident response. In emergency situations, alternative communication channels allow direct control of critical infrastructure elements without the need for intermediate services. Information probes continuously monitor user actions and suspicious requests, transmitting these data to SIEM systems for analysis and event correlation [14, 20]. Security controllers verify access rights to resources, block unauthorized requests, and maintain security levels in accordance with assigned ranks.

The architecture devotes special attention to organising confidential access to data repositories. Requests to such repositories are routed through isolated paths created by virtual private networks (VPNs) that employ tunnelling cryptography [8, 12, 13, 18, 19, 20]. This approach minimises the risks of interception, modification, or replay of data within the transmission channel. The system is

integrated with the Zero Trust security model, which operates on the principle of distrusting every component by default. Each resource access is independently validated through multi-level authorisation that includes contextual verification of user behaviour, analysis of prior actions, and interaction with incident-handling mechanisms. Acting as the analytical core, the SIEM aggregates security events, classifies them, and detects anomalies on the basis of behavioural models.

To verify the reliability of the architecture, a formalised approach grounded in cryptanalytic models is employed to estimate the probability of information disclosure, privacy degradation over time, and the effectiveness of the implemented protocols. The system incorporates mathematical mechanisms for access ranking, dynamic risk analysis, and assessment of resistance to plaintext attacks, thereby confirming its high level of cryptographic robustness [20, 22, 25, 27, 28].

Figure 5 presents an extended sequence diagram of the system that protects confidential access to information resources in computer networks, illustrating a typical interaction scenario among key components while reflecting the principles of Zero Trust, multi-factor authentication (MFA), user-behaviour analysis, and cryptographic traffic protection. The process begins when a user submits an access request through an entry point that enforces MFA and Zero Trust verification. After authentication, behaviour analysis is performed, generating a risk score that is forwarded to the Access Controller. The Access Controller conducts contextual authorisation, evaluates applicable access policies, and then issues a decision to allow or deny access. All actions are logged in the SIEM, and a denial automatically triggers an incident notification for administrators. If access is granted, a secure tunnel (WireGuard/IPsec) is established, through which data are exchanged with the information resource (Storage/API). These data remain encrypted during transit, are decrypted on the user's side, and all access events are recorded for subsequent audit. The diagram thus clearly depicts the phased execution of a secure-access scenario for confidential information, encompassing dynamic access policy enforcement, anomaly response, communication-channel protection, and centralised monitoring.

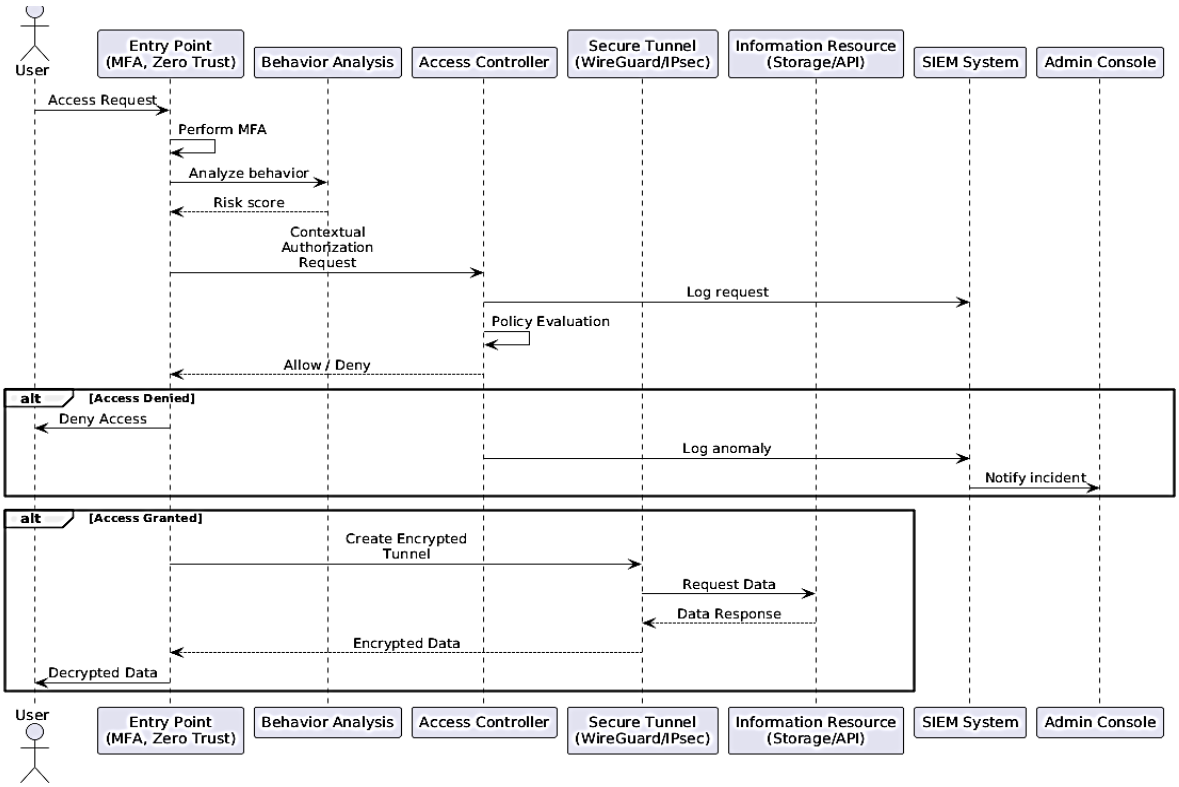

Figure 5: Sequence diagram of the architecture of a confidential access protection system with Zero Trust and behavioral analysis support

The proposed architecture is suitable for scaling and adaptation both in local area networks and in complex distributed infrastructures using cloud solutions. It allows implementing an integrated security system that maintains the confidentiality, integrity and availability of data at all levels of operation, ensuring resistance to modern threats and compliance with international information security standards.

Conclusions

The study has developed an architecture for a software system that enables confidential access to the information resources of computer networks while addressing current digital-security challenges and supporting effective interaction in highly dynamic network environments. The proposed system combines the concepts of Zero Trust, multilevel authorization, cryptographic traffic protection, and the analytical capabilities of SIEM solutions for anomaly detection and incident response. A formalized access-control model based on security ranking has been implemented, allowing the quantitative assessment of information-object security levels. The integrated mathematical mechanisms let security policies adapt in real time, taking into account risk-oriented approaches and user-behaviour factors. The incorporation of modern cryptographic protocols—TLS 1.3, IPsec, and WireGuard—guarantees resistance to transport-layer attacks, while support for multifactor authentication mechanisms ensures a high level of user trust.

Particular attention has been devoted to implementing anonymous access routes to information resources through Mix-net technology and multilevel encryption mechanisms, thereby minimizing the risk of traffic de-anonymization. Owing to its flexible, modular structure, the system can be scaled to a variety of deployment scenarios—ranging from local networks to cloud platforms—while supporting open interfaces and external software components.

The proposed architecture not only formalizes secure-access processes but also creates an adaptive environment for executing information-security strategies in real time. The system's practical value lies in its capability to integrate with existing information infrastructures and satisfy industry standards (ISO/IEC 27001, NIST SP 800-207, etc.), making it suitable for protecting critical information assets in the public, financial, educational, and medical sectors.

Thus, the study's results indicate that the developed architecture for the confidential-access software system provides a high level of information security, robust resistance to contemporary cyber threats, and the capacity to evolve further as digital-environment risks continue to develop.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] R. R. Althar, et al., Automated Risk Management based Software Security Vulnerabilities Management, in: IEEE Access 10, 2022, 90597–90608. doi:10.1109/ACCESS.2022.3185069

[2] Y. Wang, et al., Digital Transformation and Risk Management for SMEs: A Systematic Review on Available Evidence, J. Risk Financial Manag. 65(1) (2023) 209–218. doi:10.54254/2754-1169/65/20231639

[3] J. V. Barraza de la Paz, et al., A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0, Syst. 11(5) (2023). doi:10.3390/systems11050218

[4] I. Ahmad, et al., Security in Software Defined Networks: A Survey, in: IEEE Commun. Surv. Tutor. 17(4), 2015, 2317–2346. doi:10.1109/COMST.2015.2453114

[5] O. Vakhula, et al., Research on Policy-as-Code for Implementation of Role-based and Attribute-based Access Control, in: Cybersecurity Providing in Information and Telecommunication Systems (CPITS-2025), 3991, 2025 139–157.
[6] V. Susukailo, Y. Lakh, Access Control System based on Encryption in QR-Code Technology, in: IEEE 4th Int. Symposium on Wireless Systems within the Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS 2018), 2018, 158–161.
[7] H. Graupner, et al., Secure Access Control for Multi-Cloud Resources, in: IEEE 40th Local Computer Networks Conf. Workshops, 2015, 722–729. doi:10.1109/LCNW.2015.7365920
[8] B. Lipp, B. Blanchet, K. Bhargavan, A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol, in: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019, 231–246. doi:10.1109/EuroSP.2019.00026
[9] S. Ibrokhimov, et al., Multi-Factor Authentication in Cyber Physical System: A State of Art Survey, in: 21st Int. Conf. on Advanced Communication Technology (ICACT), 2019, 279–284. doi:10.23919/ICACT.2019.8701960
[10] 8 Y. Kostiuk, et al., A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2025, 249–264.
[11] Y. Kostiuk, et al., Models and Algorithms for Analyzing Information Risks during the Security Audit of Personal Data Information System, in: Cyber Hygiene & Conflict Management in Global Information Networks, 3925, 2024,155–171.
[12] H. Lee, D. Kim, Y. Kwon, TLS 1.3 in Practice: How TLS 1.3 Contributes to the Internet, in: Proc. of the Web Conf. 2021, 2568–2579. doi:10.1145/3442381.3450057
[13] B. Dowling, et al., A Cryptographic Analysis of the TLS 1.3 Handshake Protocol. J. Cryptol. 34, 37 (2021). doi:10.1007/s00145-021-09384-1
[14] M. B. M. Hata, et al., A Log Aggregation Design Criteria for Robust SIEM in Enhancing Threat Detection, in: Proc. 2023 IEEE 8th Int. Conf. on Recent Advances and Innovations in Engineering (ICRAIE), 2023, 1–6. doi:10.1109/ICRAIE59459.2023.10468438
[15] K. G. Yalda, et al., Security Issues in Software-Defined Networking (SDN) Environments, in: 23rd RoEduNet Conf.: Networking in Education and Research (RoEduNet), 2024, 1–8. doi:10.1109/RoEduNet64292.2024.10722112
[16] F. Buccafurri, et al., Achieving Sender Anonymity in Tor against the Global Passive Adversary, Appl. Sci. 12(1) (2022). doi:10.3390/app12010137
[17] N. F. Syed, et al., Zero Trust Architecture (ZTA): A comprehensive survey, in: IEEE Access 10, 2022, 57143–57179. doi:10.1109/ACCESS.2022.3174679
[18] O. Kryvoruchko, et al., Analysis of Technical Indicators of Efficiency and Quality of Intelligent Systems. J. Theor. Appl. Inf. Technol. 101(24) (2023) 127–139.
[19] S. Rzaieva, et al., Methods of Modeling Database System Security, in: Cybersecurity Providing in Information and Telecommunication Systems, 3654, 2024, 384–390.
[20] P. Skladannyi, et al., Development of Modular Neural Networks for Detecting Different Classes of Network Attacks, Cybersecur. Educ. Sci. Technol. 3(27) (2025) 534–548. doi:10.28925/2663-4023.2025.27.772
[21] Y. Kostiuk, et al., Integrated Protection Strategies and Adaptive Resource Distribution for secure Video Streaming over a Bluetooth Network, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3826, 2024, 129–138.
[22] Y. Kostiuk et al., Information and Intelligent Forecasting Systems based on the Methods of Neural Network Theory, in: Proc. Smart Information Systems and Technologies (SIST), 2023, 168–173. doi:10.1109/SIST58284.2023.10223499
[23] F. A. Qazi, Study of Zero Trust Architecture for Applications and Network Security, in: IEEE 19th Int. Conf. on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), 2022, 111–116. doi:10.1109/HONET56683.2022.10019186

[24] Y. Kostiuk, et al., Information Protection and Secure Data Exchange in Wireless Mobile Networks with Authentication and Key Exchange Protocols, Cybersecur. Educ. Sci. Technol. 1(25) (2024), 229–252. doi:10.28925/2663-4023.2024.25.229252
[25] L. Chen, et al., Security-Enhanced WireGuard Protocol Design Using Quantum Key Distribution, in: Proc. 2024 Int. Conf. on Computing, Networking and Communications (ICNC), 2024, 718–723. doi:10.1109/ICNC59896.2024.10556292
[26] S. Al-Shareeda, F. Özgüner, Preserving Location Privacy using an Anonymous Authentication Dynamic Mixing Crowd, in: Proc. 2016 IEEE 19th Int. Conf. on Intelligent Transportation Systems (ITSC), 2016, 545–550. doi:10.1109/ITSC.2016.7795607
[27] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, 3421, 2023, 97–106.
[28] R. Syrotynskyi, et al., Methodology of Network Infrastructure Analysis as Part of Migration to Zero-Trust Architecture, in: Cyber Security and Data Protection, 3800, 2024, 97–105.