Ingénierie des Systèmes d'Information
Vol. 31, No. 8, August, 2026, pp. 2697-2713
Journal homepage: http://iieta.org/journals/isi

Process-Aware Contextual Access Control Framework Integrating Role-Based Authorization for Secure Information Systems

Askhat Ryspayev

Center for Military-Strategic Research, Joint Stock Company, Astana 010000, Kazakhstan

Corresponding Author Email: askhatryspayev@cvsi.kz

https://doi.org/10.18280/isi.310816

Received: 29 April 2026
Revised: 11 August 2026
Accepted: 20 August 2026
Available online: 31 August 2026

Keywords:
process-aware authorization, context-aware access control, Role-Based Access Control, information-system security, Zero Trust Architecture, adaptive security

ABSTRACT

Cyber threats against enterprise information systems have increased the demand for adaptive access-control mechanisms capable of responding to dynamic operational conditions. Traditional Role-Based Access Control (RBAC) models provide efficient permission management but often lack contextual awareness and workflow-level validation, which limits their ability to prevent misuse of legitimate privileges. This study proposes a Process-Aware Contextual Access Control Framework that integrates role-based authorization, contextual risk evaluation, workflow-state validation, encryption protection, and continuous security monitoring into a unified security architecture. The proposed framework extends conventional RBAC by introducing workflow state as an additional authorization factor rather than treating process monitoring as an independent security function. A prototype system was implemented using OAuth 2.0, JSON Web Tokens (JWT), Advanced Encryption Standard (AES)-256 encryption, Transport Layer Security (TLS) 1.3 communication, and policy-based access management. The framework was evaluated through penetration testing, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat analysis, and performance benchmarking against a conventional RBAC model. Experimental results show that the proposed framework reduces successful attack attempts under credential theft, session hijacking, privilege escalation, and unauthorized workflow operations while maintaining acceptable computational overhead. The findings demonstrate that combining contextual assessment with process-aware authorization provides more adaptive access decisions for enterprise information systems. Although the prototype was validated under controlled experimental conditions, further evaluation using large-scale enterprise environments is required to assess scalability and deployment feasibility.

1. INTRODUCTION

The rapid adoption of digital infrastructures, cloud computing environments, and distributed enterprise systems has significantly increased cyber threats targeting information systems. The increasing use of automated workflows, shared databases, and process APIs has become essential for modern enterprises, making access control a critical component of information-system security. Although automated workflows, shared databases, and API-oriented services improve operational efficiency, they also introduce significant security risks that require robust access-control mechanisms.

Insufficient access control can lead to privacy breaches, privilege abuse, process manipulation, data compromise, and operational disruption. Traditional security architectures primarily rely on perimeter-based protection and static permission models, making them vulnerable to modern attacks that exploit insider threats, compromised credentials, and privilege escalation.

Role-Based Access Control (RBAC) is one of the most popular authorization systems due to its ability to assign roles to users, which makes managing permissions for users easy.

However, traditional RBAC does not provide dynamic flexibility, situational awareness, and process-level authentication. Attackers can use static permissions through privilege escalation, session hijacking, or insider abuse.

Attribute-Based Access Control (ABAC) addresses some of these limitations by incorporating contextual attributes into access decisions; however, this increased flexibility is often accompanied by greater policy complexity and computational overhead.

Zero Trust Architecture (ZTA) deals with continuous verification but may not be based on well-organized RBAC. Business Process Management (BPM) systems improve workflow monitoring and execution but are generally not tightly integrated with authorization mechanisms.

A failure to adhere to the concept of integrating role-based authorization and process-driven security intelligence is one of the biggest scientific uncertainties. The existing models also focus on access control, authentication, encryption, and workflow validation as separate modules instead of being one of the components of the security architecture.

This fragmented design can result in inconsistent policy enforcement, delayed threat detection, and limited visibility

across security operations. Although considerable progress has been made in RBAC, ABAC, ZTAs, and workflow-security frameworks, these approaches primarily address individual dimensions of system security rather than providing a unified authorization model.

Existing hybrid architectures generally combine role and contextual information but rarely incorporate workflow-state validation as a core component of access decisions. Moreover, encryption, continuous monitoring, and process validation are commonly implemented as supporting security services instead of being integrated directly into the authorization mechanism. Consequently, a unified framework capable of simultaneously evaluating user identity, assigned roles, contextual conditions, workflow state, and continuous security monitoring remains insufficiently explored in the current literature.

Secure Role-Based Information System (SRBIS) offers real-time, adaptive protection, which satisfies the needs of modern enterprises by combining formal access modelling, layered security controls, and dynamically analyzing threats.

Unlike conventional access-control approaches that primarily focus on static permission assignment or isolated attribute evaluation, SRBIS introduces a process-aware authorization mechanism that incorporates workflow states and contextual conditions into access decisions, enabling adaptive protection against privilege misuse, credential compromise, and context-dependent threats.

To address this research gap, this study proposes the SRBIS, an adaptive access-control architecture that integrates role-based authorization, contextual validation, workflow-state awareness, encrypted communication, and continuous monitoring into a unified security framework.

The primary novelty of SRBIS lies in the integration of process-state awareness with contextual and role-based authorization within a unified access decision mechanism.

Existing RBAC models primarily rely on predefined roles and permissions, while ABAC-based approaches extend authorization through environmental attributes but often lack explicit consideration of business workflow states.

Similarly, ZTAs emphasize continuous verification but generally operate at the identity and network-security level rather than incorporating process execution constraints into authorization decisions.

SRBIS addresses this limitation by introducing a process-aware adaptive authorization model in which access decisions are dynamically determined through the combined evaluation of user identity, assigned role, permission requirements, contextual conditions, and current workflow state.

Unlike conventional hybrid approaches that combine RBAC and ABAC attributes, SRBIS treats process state as an independent authorization factor, allowing the system to prevent legitimate users from performing unauthorized actions even when valid credentials and permissions exist. Therefore, the contribution of SRBIS is not merely the combination of existing security components but the development of a unified decision-making architecture that links role management, contextual risk evaluation, and workflow integrity into a single and adaptive authorization process.

To clarify the nature of this contribution, SRBIS should be understood as an integrated authorization decision mechanism rather than as a fundamentally new access-control theory.

The decision mechanism operates through sequential and conjunctive validation of five authorization dimensions: authenticated user identity, role and permission eligibility, contextual risk conditions, current workflow state, and policy constraints.

A request is authorized only when the role-permission requirements are satisfied, the contextual risk remains within the permitted threshold, and the requested operation is valid for the current workflow state.

Thus, the distinctive decision logic of SRBIS is the use of workflow state as an active authorization condition that can override otherwise valid role and permission assignments.

This mechanism enables SRBIS to distinguish between a user who is generally authorized to perform an operation and a user who is authorized to perform that operation under the specific contextual and process conditions prevailing at the time of the request.

Accordingly, the novelty claimed in this study concerns the integration and operationalization of this process-aware, context-aware decision mechanism within a unified enterprise security architecture, rather than the invention of new RBAC, ABAC, Zero Trust, or cryptographic primitives.

The main contributions of this study are as follows:

Process-aware adaptive authorization model: SRBIS introduces a unified access decision mechanism that extends traditional RBAC by incorporating workflow states as an additional authorization factor alongside roles, permissions, and contextual attributes.

Context-aware threat detection: SRBIS dynamically evaluates environmental and behavioral conditions, including device trust, network integrity, and session characteristics, to adjust authorization decisions according to real-time risk conditions.

Performance-efficient design: SRBIS demonstrates that process-aware and context-aware authorization can improve security resilience while maintaining acceptable computational overhead through layered security enforcement.

Better resilience of the enterprise: The framework offers adaptive security that improves resistance, responsiveness, and continuity of operation in distributed enterprise settings.

This combined solution shows obvious benefits compared to the classic RBAC and ABAC designs, which offer real-time and adaptive security that is viable and effective for modern enterprise systems.

The architecture is designed to improve security resilience while maintaining acceptable system performance. The solution is a blend of formal access modelling, layered architecture, and real-time threat monitoring to provide adaptive security of an enterprise environment.

The proposed framework demonstrates how integrating adaptive authorization with process intelligence can improve system resilience, threat detection, and response efficiency.

2. LITERATURE REVIEW

2.1 Evolution of access control models

Access-control mechanisms constitute a fundamental component of information-system security by ensuring that unauthorized users cannot access protected resources [1]. Early discretionary and mandatory access-control models primarily focused on static permission assignment, limiting scalability and administrative efficiency in complex organizational environments [2].

RBAC brought a new paradigm as it abstracted the

permissions into roles instead of allocating them to users directly. The approach boosted control, reduced duplication of the policies, and aligned the privileges of the system with the designs of the organizations [3, 4]. However, classical RBAC models lack a dynamic and contextually varied environment with a changing threat profile, thus cannot be applied to such environments [5, 6]. Researchers have indicated that the existing static permission architecture is inappropriate in managing dynamic risk scenarios and needs dynamic, context-based authorization procedures [7, 8].

2.2 Advances in context-aware and attribute-based security

To overcome the limitations of fixed role assignments, recent research has increasingly focused on ABAC and context-aware security models.

These are techniques that rely on environmental parameters like device identities, location, time, and behavioral patterns to authorize access [9, 10]. Context-aware mechanisms allow systems to dynamically determine trust conditions, and hence, prior to access, thus reducing the likelihood of unauthorized activity occurrence [11, 12].

According to the literature, attribute-based models tend to be more lenient and more granular than role-based systems, but also come with their own complexity of policies, computational requirements, and rule management.

The increasing amount of contextual information also makes decision-making more difficult [13], and requires effective evaluation algorithms and scalable structures [14, 15]. Later studies of the era suggest a mixed mode that combines role structures and situational validation to balance administrative simplicity and adaptive security [16, 17].

2.3 Integration of zero-trust principles in information systems

The Zero Trust paradigm is among the most popular security philosophies for contemporary digital infrastructures, particularly in cloud-based and distributed computing environments.

Unlike the traditional security framework that relied on a perimeter security model, Zero Trust assumes that no user or device can be trusted in principle, including within the network [18, 19]. The primary concepts of this model are constant authentication, high-level validation, and least-privilege implementation.

Empirical evidence indicates that Zero Trust design significantly reduces attack surfaces and improves visibility into lateral movement within systems [20, 21].

Nevertheless, current implementations are usually more concerned with network-level security and identity authentication, but pay little attention to workflow integrity and process-level authorization [22, 23].

This weakness indicates that Zero Trust should be combined with formal access mechanisms to ensure the security of the entire system, including both information and business operations [24].

2.4 Secure process management and workflow protection

BPM systems are important to the organization's operations because they automate workflows and ensure coordination among users, applications, and databases [25].

As these systems become increasingly digitalized, they are more frequently targeted by attacks that manipulate business-process logic or exploit workflow execution [26, 27].

Studies on secure workflow management underscore the importance of tracking process states, validating transactions, and handling anomalies during execution [28, 29]. Models offered include logging and auditing features, which are not always directly integrated with access control engines.

Consequently, decisions regarding authorized workflow may not be informed by prevailing workflow conditions; thus, they can be easily compromised.

Recent studies suggest having process-aware security architectures where authorization policies are coupled with the workflow state, and systems can respond to unauthorized actions even when valid credentials are used by users [30, 31].

2.5 Research gap and emerging hybrid frameworks

Despite significant advances in RBAC, ABAC, Zero Trust, and workflow-security research, existing approaches continue to address adaptive authorization from different perspectives rather than through a unified decision model.

Hybrid access-control architectures generally combine user roles with contextual attributes, whereas workflow-security models primarily protect business-process execution independently of authorization.

Consequently, relatively little research has investigated access-control frameworks that integrate workflow-state validation directly into the authorization decision process. This unresolved limitation constitutes the primary research gap addressed by the proposed SRBIS framework.

The solutions in place lack built-in identity validation, role authorization, contextual encryption, and process monitoring features, but concentrate on individual security levels [32].

This separation results in delayed threat detection, inconsistent policy enforcement, and limited situational awareness. Trends in current research suggest that there is a need to have integrated architectures that can be used to concurrently analyze the user roles, environmental conditions, and process states [33]. The advantage of these hybrid systems is that they will be stronger against high-level attacks, be more transparent in their work, and respond better to incidents.

However, not a lot of detailed models defining and experimentally illustrating this integration are generally in circulation, and this is why further studies are necessary on integrating SRBISs. In order to give a more analytical comparison, Table 1 summarizes some of the important features of the discussed models of access control.

Table 1 indicates the strengths and weaknesses of each model concerning context awareness, scalability, workflow awareness, and security effectiveness.

Table 1. Comparison of the models of access control, emphasizing their main features and constraints

Access Control Model	Context Awareness	Scalability	Workflow Awareness
RBAC	Low	High	Low
ABAC	High	Moderate	Low
Zero Trust	Moderate	High	Moderate
Hybrid / Mixed	High	Moderate	Low

Note: RBAC = Role-Based Access Control, ABAC = Attribute-Based Access Control, SRBIS = Secure Role-Based Information System.

This analogy highlights the missing links in current

strategies. It is evident that this shows the newness of the proposed SRBIS architecture, which brings together role-based authorization, contextual assessment, and workflow monitoring in a single architecture.

This comparison highlights the unresolved integration gap addressed by SRBIS, particularly the direct incorporation of workflow-state validation into the authorization decision process.

Recent research has increasingly focused on hybrid RBAC–ABAC architectures to balance administrative simplicity with adaptive authorization. These studies demonstrate that contextual attributes such as device trust, user behavior, temporal constraints, and environmental conditions can significantly improve access-control accuracy compared with static role assignments.

Nevertheless, most hybrid models continue to evaluate contextual information independently of workflow execution, leaving process-state validation largely outside the core authorization mechanism.

2.6 Related work

The importance of access control in information-system security is well established, and RBAC continues to be widely studied as an effective model for mapping permissions to organizational roles.

The main benefit of RBAC is that it offers a formal representation of the roles and permissions, and as such, is comparatively easy to manage policies and enhance auditability.

The newest work [34] discusses the evolution of RBAC in the context of cloud security governance and outlines how conventional RBAC can be improved with smart capabilities, i.e., artificial intelligence, to identify threats, streamline roles, handle security threats, and improve regulatory compliance in multifaceted infrastructures, or in cloud-based environments.

Though RBAC is useful in simple authorization, the notion of ABAC has been suggested to overcome the limitation of RBAC as a fixed control by using a multidimensional set of attributes in the determination of access.

A study by Atlam and Yang [35] provides in-depth research on ABAC in business. It indicates that attribute-based controls will put it at ease, context-aware and adaptive in dynamic cloud and IoT environments.

In this case, where it is necessary to determine the environmental, resource, and subject attributes in a single operation, ABAC allows finer-grained security policies to be implemented, especially when traditional role assignments cannot offer access criteria of any finer granularity.

Zero Trust principles used in access-control architecture have received a lot of research studies due to the fact that it lays emphasis on the saying never trust, always verify.

An example of an efficient Zero Trust-based dynamic access control framework for cloud computing offered by Al-Ahmad et al. [33] is that user trust scores are actively calculated and the access policy is dynamically updated, which is more responsive and adaptable to the conditions of threat than traditional approaches.

They highlight in their work the need to combine continuous authentication and the flexibility of rule modification to ensure a secure deployment in the cloud ecosystem, where the resources and threat boundaries are quickly changing.

The alternative, influential trend in access control study is hybrid models, which are RBAC-based, ABAC-based, and continuous monitoring within the Zero Trust setup.

A strength of the study [36] is that the model presents a longer access control model, which integrates the concepts of Zero Trust with RBAC and ABAC to support conditional access and ongoing monitoring of user activity, which is more responsive to insider and outsider threats, as compared to standalone models.

Such integrated models have the objectives of mediating administrative simplicity of RBAC and the context sensitivity of ABAC in a highly secure operating environment. Although IoT research demonstrates the importance of adaptive access control in resource-constrained environments, its primary emphasis is on scalability, lightweight authentication, and decentralized communication.

Since the present study focuses on enterprise information systems rather than IoT infrastructures, these studies are referenced only to illustrate the broader evolution of adaptive authorization mechanisms rather than as direct design foundations of SRBIS.

It presents a secure and scalable IoT access control framework that integrates dynamic attribute updates and policy hiding with attribute-based encryption, showing that real-time policy updates can enhance the security and confidentiality of data in a decentralized network.

As evidenced in this paper, advanced access control plans are not limited to enterprise-level data systems, but they are also required in next-generation IoT implementations. Blockchain-based access-control mechanisms have been proposed primarily for decentralized environments where immutable audit trails and distributed trust are required.

Although these approaches improve transparency and tamper resistance, they introduce additional computational overhead and are generally designed for decentralized infrastructures rather than enterprise role-based information systems. Consequently, blockchain technologies are considered complementary rather than central to the proposed SRBIS architecture.

The papers of access control based on blockchain in cloud computing [7, 16] conclude that with the use of a decentralized ledger and access control, trust, transparency, and tamper-resistant log-keeping in cloud and hybrid systems can be enhanced.

Overall, the literature indicates a clear progression from static role-based authorization towards adaptive, context-aware, and continuously verified access-control architectures.

Nevertheless, relatively few studies integrate workflow-state validation directly into the authorization decision process.

This limitation represents the principal research gap addressed by SRBIS through its unified integration of role management, contextual evaluation, process-state awareness, and continuous security monitoring.

This is demonstrated by the fact that Mao, in actuality, designed a Zero Trust access control model in relation to the use of attribute and dynamic trust scores, and owing to this fact, constant trust assessment built into ABAC is able to provide access to real-time trustworthiness, hence the higher throughput and accuracy than conventional ABAC methods.

This highlights the increased necessity to add trust assessment mechanisms into access control systems, especially in cloud systems and distributed systems.

Recent application research is on access control in specific environments, including university management systems and smart environments.

RBAC and ABAC in Zero Trust for university systems, demonstrating that hybrid systems can offer institutional data security without loss of flexibility or policy flexibility. This type of domain-based research stresses that with no loss of security rigor, hybrid models can be scaled to application needs.

The other active field is in sophisticated cryptography measures to aid in the access control process. Other authors have also reported the use of attribute-based models in conjunction with smart contracts and immutable logs in a decentralized setting, and have indicated greater resilience to attribute disclosure and unauthorized access through cryptographically protected attributes and transaction histories.

The above approaches show that cryptographic support can supplement access control rules by ensuring that sensitive credentials and historical attributes are written with integrity guarantees that cannot be reversed.

To provide a more analytical evaluation, each STRIDE threat was assessed according to its estimated likelihood and operational impact before and after implementation of the proposed SRBIS architecture (Table 2).

Risk severity was categorized as High, Medium, or Low based on the probability of successful exploitation and the expected consequences for confidentiality, integrity, and availability.

Following implementation of layered authentication, contextual validation, workflow-state verification, encryption, and continuous monitoring, all initially high-risk threats were reduced to low residual risk, whereas Denial-of-Service attacks remained at medium residual risk because complete prevention depends on external network-level protection mechanisms.

The STRIDE assessment demonstrates that the greatest security improvements were achieved against identity-based attacks, particularly credential theft and privilege escalation.

These attack categories are effectively mitigated because SRBIS requires successful verification of user identity, contextual conditions, workflow state, and policy constraints before authorizing access.

In contrast, Denial-of-Service attacks can't be eliminated entirely through access-control mechanisms because they primarily target system availability rather than authorization logic.

Consequently, SRBIS significantly reduces authentication and authorization risks while remaining dependent on complementary network-level defense mechanisms for availability protection.

Table 2 demonstrates that existing access-control approaches generally emphasize one or two security dimensions, such as role assignment, attribute evaluation, or continuous verification.

Table 2. STRIDE risk analysis of SRBIS

STRIDE Threat	Affected Module	Risk Before Mitigation	Mitigation Implemented	Residual Risk
Spoofing	Identity & Authentication	High	MFA + OAuth 2.0 + JWT	Low
Tampering	Encryption Layer	High	AES-256 + TLS 1.3	Low
Repudiation	Audit Logging	Medium	Immutable Audit Logs	Low
Information Disclosure	Policy Engine	High	Context-aware Authorization	Low
Denial of Service	Process Controller	Medium	Request Throttling + Validation	Medium
Elevation of Privilege	Context Analyzer	High	Multi-factor Context Validation	Low

Note: MFA = multi-factor authentication, JWT = JSON Web Tokens, AES = Advanced Encryption Standard, TLS = Transport Layer Security, SRBIS = Secure Role-Based Information System, STRIDE = Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

However, they rarely integrate workflow-state validation directly into the authorization decision process.

In contrast, SRBIS combines role management, contextual risk evaluation, workflow-state verification, encryption, and continuous monitoring within a unified adaptive authorization architecture.

This integrated design distinguishes SRBIS from existing RBAC, ABAC, Zero Trust, and hybrid access-control approaches.

3. METHODOLOGY

3.1 Formal access model

SRBIS extends the traditional RBAC model by integrating contextual validation and workflow-aware authorization into the access decision process, incorporating contextual access validation and process-aware authorization.

The distinctive aspect of the SRBIS model is that workflow state (T) is not treated as an operational monitoring parameter but as an active authorization factor. The SRBIS decision mechanism follows a conjunctive authorization logic in which role-based eligibility is necessary but not sufficient for access.

First, the system authenticates the requesting user and verifies the user's assigned role and requested permission. Second, the Context Analyzer evaluates runtime conditions and derives a contextual risk value from device trustworthiness, network integrity, session freshness, and related behavioral indicators. Third, the Process Management Controller verifies whether the requested operation is permitted in the current workflow state. The final authorization decision is therefore generated from the joint satisfaction of identity, role-permission, contextual-risk, and workflow-state conditions.

If any mandatory authorization condition fails, the request is denied or subjected to additional verification, even when the user possesses otherwise valid credentials and permissions.

This sequential-conjunctive mechanism constitutes the operationally distinctive feature of SRBIS because it makes process-state validity a mandatory part of authorization rather than an external workflow-monitoring function.

This enables the system to evaluate whether a requested action is permissible within the current process stage, even when the user possesses valid credentials and assigned permissions.

It is formally defined as the mechanism for access decisions.

$$Access = f(U, R, P, C, T) \quad (1)$$

where,

•U denotes the authenticated user identity;

•*R* represents the assigned role;
•*P* denotes the permission set;
•*C* represents contextual attributes;
•*T* denotes the current process state.

Importantly, the contextual risk score does not independently determine authorization. Instead, it functions as one decision input within the broader SRBIS authorization mechanism. A low contextual risk cannot compensate for an invalid role-permission assignment or an invalid workflow state, while a valid role and permission cannot compensate for a failed contextual or process-state condition.

The final decision therefore follows a mandatory multi-condition logic in which contextual risk operates as an adaptive constraint and workflow state operates as a process-integrity constraint. This distinction is central to the SRBIS contribution: the framework does not simply aggregate RBAC and ABAC characteristics, but establishes a decision sequence in which process-state validity is explicitly coupled with role, permission, and runtime-context validation before protected resources can be accessed.

Authorization is granted only after all variables meet the predetermined policy constraints. In contrast to traditional RBAC models that treat a large portion of credential validation as a statistical matter, the proposed algorithm dynamically assesses runtime conditions and workflow stages, thereby eliminating the concept of unauthorized operations when valid credentials are presented. Role hierarchy is defined as:

$$R_i \geq R_j \Rightarrow \text{Perm}(R_i) \supseteq \text{Perm}(R_j) \quad (2)$$

It is a setup that is hierarchical and allows transfer of the permissions of lower role positions, but at the same time, high enforcement of policies.

The contextual validation role is represented as:

$$Cvalid = Dt \wedge Ni \wedge Sf \quad (3)$$

where,
•*Dt* denotes device trustworthiness;
•*Ni* denotes network integrity;
•*Sf* denotes session freshness.
The final authorization rule is:

$$Grant \Leftrightarrow (Rolevalid \wedge Cvalid \wedge Pvalid) \quad (4)$$

The multi-factor decision mechanism ensures that authorization depends not only on user identity but also on contextual conditions and workflow status.

The proposed secure RBAC algorithm ensures that users are granted or denied access based on their authenticated roles and contextual evaluation, as illustrated in Figure 1.

3.2 System architecture

The proposed system architecture is a multi-layered, modular, and security-oriented framework comprising six integrated components that provide secure, context-aware, and process-aware access control.

This architecture does not use traditional access control systems that rely on credential verification as the primary approach; rather, it adopts a defense-in-depth paradigm in which authorization decisions are authenticated across a series of independent security levels before access to system resources is granted. The modules have their functional specialization while interacting with one another through secure interfaces, forming a resilient, fault-tolerant ecosystem that can withstand external and internal threats.

This module authenticates users using multi-factor authentication (MFA), cryptographic credentials, and secure session validation. In addition to determining access permission, a successful authorization decision activates the cryptographic service responsible for secure data retrieval.

Consequently, access approval and data decryption are sequential operations within the same security workflow, preventing encrypted information from being exposed to unauthorized users even if storage media or communication channels are compromised.

3.2.1 Identity and authentication module

This module is the primary access point for any access request and authenticates user identities using MFA settings.

It combines password-based authentication, one-time authentication, biometric authentication, and cryptographic authentication keys to guarantee high identity assurance.

The token validation schemes recognize the authenticity of a session and eliminate replay and impersonation attacks.

This module also manages the session lifecycle, e.g., token expiration, renewal, and revocation, so that only authenticated and authorized users can initiate the system. The authentication module was implemented using the OAuth 2.0 authorization framework with JSON Web Tokens (JWT) for stateless session management.

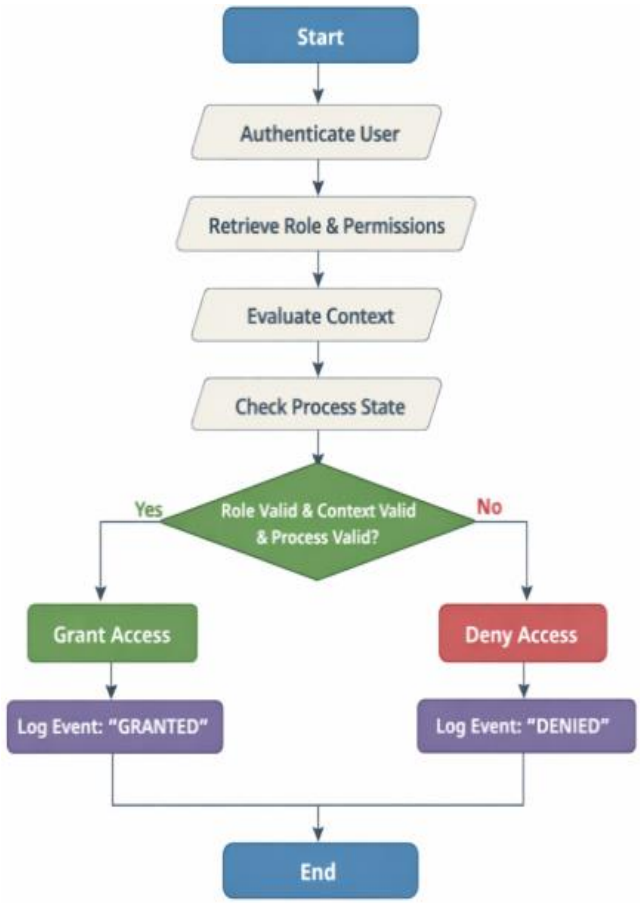

Figure 1. Workflow of the proposed Secure Role-Based Information System (SRBIS) access-control algorithm showing identity authentication, role verification, contextual validation, workflow-state evaluation, and final authorization decision

User credentials were verified through encrypted password hashes using the BCrypt algorithm, after which a signed JWT containing user identity, assigned roles, and session metadata was generated. MFA required successful password verification followed by a one-time authentication code before an access token was issued. Session expiration, token renewal, and token revocation were managed automatically through server-side validation.

3.2.2 Role and Policy Engine

The Role and Policy Engine is the central point of decision-making in the architecture. It enforces a hierarchy of roles, permission mappings, and policy rule sets, allowing authorized operations for each type of user.

This sub-module is a dynamic component that authorizes requests through user role authentication, compares the user role against the associated privileges, and applies policy constraints such as separation of duties, least privilege, and role inheritance.

Real-time updates on policies are also supported by the engine so that administrators can modify access rules without influencing the work of the system and make the system more dynamic and effective for administration.

Authorization policies were stored in relational policy tables within PostgreSQL. Each incoming request triggered a policy evaluation that matched the authenticated user role with the requested resource and operation.

The policy engine further enforced least-privilege constraints, role inheritance, and separation-of-duty rules before generating an authorization decision.

Policy evaluation required only indexed database lookups, resulting in low computational overhead during runtime.

3.2.3 Context Analyzer

The Context Analyzer is one of the systems that adds environmental and situational awareness to the authorization decisions to facilitate better system security.

It keeps analyzing the geographic position of the device, fingerprints, context information, IP reputation ratings, behavior during the session, and behavioral irregularities.

Once these parameters have been analyzed, the system is able to identify suspicious activity, including an attempt to log in with an unknown device or at an odd time.

It intervenes by instigating further checks or denying connections.

This contextual analysis transforms static authorization into an adaptive decision process capable of responding to changing security conditions.

Consequently, the system will guard against loss of data, integrity of business logic, and consistency in operations as well. As illustrated in Figure 2, the Context Analyzer workflow demonstrates these processes and their interactions.

Contextual validation was performed by evaluating four runtime attributes: (i) registered device fingerprint, (ii) network trust level based on IP reputation and Transport Layer Security (TLS) session integrity, (iii) login time and geographical consistency with previous sessions, and (iv) behavioral indicators including repeated authentication failures and abnormal access frequency. Each attribute contributed to a weighted contextual risk score ranging from 0 to 100. Requests exceeding the predefined security threshold triggered additional authentication or were rejected automatically.

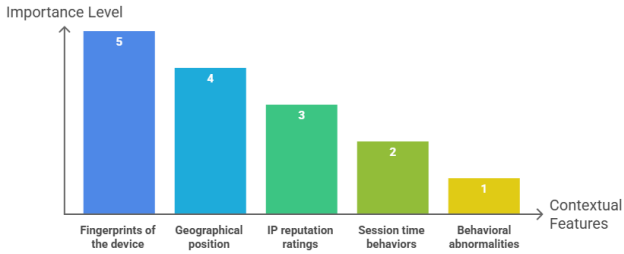

Figure 2. Operational workflow of the Context Analyzer illustrating device verification, IP reputation analysis, behavioral assessment, contextual risk calculation, and adaptive access decision

Figure 3. Integrated encryption workflow demonstrating secure key management, Advanced Encryption Standard (AES)-256 data encryption, Transport Layer Security (TLS) 1.3 communication, and cryptographic protection during the Secure Role-Based Information System (SRBIS) authorization process

3.2.4 Encryption Layer

The Encryption Layer provides data confidentiality and integrity across all system operations. Unlike conventional architectures where encryption operates independently of authorization, the proposed SRBIS integrates cryptographic protection directly into the access-control workflow.

Data decryption is performed only after successful completion of identity authentication, role verification, contextual validation, and workflow-state confirmation. Consequently, encryption functions as an additional enforcement layer within the authorization process rather than as an isolated security mechanism.

Following successful authorization by the Role and Policy Engine, the Encryption Layer retrieves the appropriate cryptographic key to decrypt only the specific data resources permitted by the approved access policy.

If authentication or contextual verification fails at any stage, decryption is not initiated and encrypted data remain inaccessible. This design ensures that cryptographic protection and access-control decisions operate as a unified security mechanism. It secures the stored and transmitted information with advanced cryptographic algorithms, secure key management protocols, and encrypted communication channels. Strong symmetric encryption is used to secure data at rest, and secure transport protocols are used to secure data in transit, ensuring it cannot be intercepted or tampered with. The overall workflow of the Encryption Layer is illustrated in

Figure 3. Data stored in PostgreSQL was encrypted using Advanced Encryption Standard (AES)-256 symmetric encryption before persistence. Cryptographic keys were securely managed using protected server-side key storage and were never transmitted to clients.

Communication between clients and the application server employed TLS 1.3 with ephemeral session keys to guarantee confidentiality and forward secrecy during data transmission.

3.2.5 Process Management Controller

This part brings workflow awareness to the access control mechanism. It tracks the state changes of the processes and confirms the legitimacy of the requested actions of the right workflow phases.

Although a user may possess valid credentials and permissions, access is denied if the requested operation violates workflow constraints or falls outside the authorized execution stage.

Process-aware validation ensures that authorized users perform only those actions permitted within the current workflow stage, thereby protecting business-process integrity.

As a result, the system also protects against data loss, the integrity of business logic, and operational consistency.

3.2.6 Audit and Logging Module

The Audit and Logging Module offers much control and insight into what is occurring in the system.

It records authentication events, authorization decisions, policy updates, system anomalies, and user activities in tamper-resistant audit logs.

These records can be used to conduct forensic investigations, accountability allocation, incident response, and security investigations.

The module also has automated alert systems that inform administrators in real-time about suspicious or policy-violating activity to quickly identify and prevent any possible threat.

3.2.7 Security paradigm in architecture

The overall design is a layered validation, where each layer is allowed to validate certain security requirements prior to passing a request to the subsequent layer.

Access is granted after all the modules have confirmed that the identity, role permission, contextual requirements, cryptographic integrity, process legitimacy, and audit requirements have been satisfied.

This distributed verification model eliminates single points of failure and enhances system resilience against complex threats, including privilege escalation, session hijacking, insider misuse, and advanced persistent threats (APTs).

The stepwise authorization flow is as follows:

Identity module: checks user credentials and identity of the requester;

Policy engine: compares the roles and permissions of the user with the access policies;

Context Analyzer: verifies the context, such as device fingerprint, location, time, and behavior patterns;

Process controller: verifies the validity of the process requested, confirms that the workflow is correct, and keeps audit trails;

Access decision: after all the modules have passed their verification, access is denied or granted based on the aggregate verification.

The sequential architecture should not be interpreted as a simple collection of independent security modules. Its distinguishing feature is the dependency among the authorization stages: the output of each validation stage becomes a prerequisite for the subsequent decision stage.

In particular, workflow-state validation is coupled with role-permission and contextual validation rather than being performed only for monitoring or auditing purposes.

Consequently, a request that satisfies identity and role requirements can still be rejected when its contextual risk exceeds the permitted threshold or when the requested operation is inconsistent with the current process state.

This dependency transforms workflow awareness from a supporting security function into an enforceable authorization condition.

Figure 4 shows the layered security paradigm and the sequential discussions between these modules when authorizing a request.

Figure 4. Layered Secure Role-Based Information System (SRBIS) security architecture illustrating sequential validation across authentication, policy evaluation, contextual analysis, workflow verification, encryption, and audit logging modules

3.3 Technical implementation

The SRBIS prototype was implemented using a client–server architecture. The backend application was developed using Python, while PostgreSQL served as the relational database management system.

User authentication was implemented through OAuth 2.0 with JWT, and passwords were protected using BCrypt hashing.

AES-256 encryption secured sensitive information stored in the database, whereas TLS 1.3 protected all client–server communication.

Access-control policies were evaluated dynamically through PostgreSQL policy tables containing role assignments, permissions, contextual constraints, and workflow-state rules.

The Context Analyzer continuously evaluated runtime attributes including device fingerprint, IP reputation, session freshness, geographical consistency, and behavioral anomalies before calculating a contextual risk score.

Workflow validation was implemented through predefined process-state transition rules enforced before every protected operation.

Security events were recorded within tamper-resistant audit logs and analyzed continuously to support anomaly detection and incident response.

3.4 Evaluation methods

The integrated evaluation strategy was designed to simulate realistic operational environments while enabling a systematic comparison with conventional access-control architectures.

All the evaluation methods consider a different aspect of system reliability. As such, it is ensured that inferences about effectiveness and efficiency are both scientifically and practically sound.

3.4.1 Penetration testing

Controlled penetration testing was performed using a predefined attack framework designed to simulate realistic enterprise cyber threats.

Four representative attack categories credential theft, session hijacking, privilege escalation, and insider unauthorized operations – were executed against both the baseline RBAC implementation and the proposed SRBIS framework.

Each attack scenario consisted of 100 independent attack attempts under identical system configurations. Successful attacks were recorded when unauthorized access or unauthorized process execution was achieved. All experiments were repeated ten times to minimize random variation and improve statistical reliability.

The evaluation included multiple attack vectors, including credential spoofing, privilege escalation, session hijacking, and injection-based attacks, executed within a controlled testing environment.

This method allowed direct assessment of the system defense power, its resistance to attacks, and the performance of the anomaly detection.

3.4.2 STRIDE-based threat modeling

Threat modeling was performed systematically, with the help of the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege): it was possible to systematically identify the possible vulnerabilities in different architectural layers through the use of the framework.

All the system modules were taken into consideration to identify the potential attack surfaces, threat probability, and the impact that will be incurred. Unlike a conventional STRIDE checklist, the proposed evaluation assessed the relative security risk associated with each threat category before and after implementation of SRBIS.

This analytical assessment enabled identification of the threats that benefited most from contextual validation, workflow-state verification, and adaptive authorization while also highlighting residual risks requiring complementary security controls.

The expanded attack evaluation demonstrates that SRBIS provides protection across multiple categories of security threats rather than only identity-based attacks.

Authentication attacks, privilege abuse, replay attacks, database attacks, and unauthorized API requests were successfully prevented through the combined operation of contextual validation, policy enforcement, encrypted communication, and workflow-state verification.

Table 3 summarizes the threats identified, the modules/components evaluated, possible vulnerabilities, and the mitigation measures.

Although request throttling reduced the impact of Denial-of-Service attacks, complete mitigation of large-scale network flooding remains dependent on complementary infrastructure-level security mechanisms such as firewalls and load balancers.

3.4.3 Performance benchmarking

A performance test under controlled workloads was conducted to assess computational efficiency, scaling, and responsiveness [37].

Benchmarking experiments were performed to determine the latency, as well as throughput and processing stability, when the load of the requests was variable and when the users were operating simultaneously.

Stress tests were also done to determine the behavior of the system when operating at peak conditions.

Such experiments validated the existence or nonexistence of overheads in performance due to the additional security measures and the acceptable overheads within the functionality boundaries of deployment on a large scale.

Performance evaluation was conducted under controlled laboratory conditions to ensure repeatability and consistency. The prototype was deployed on a workstation equipped with an Intel Core i7 processor (3.40 GHz), 16 GB RAM, and Ubuntu 22.04 LTS.

The application server was implemented using Python 3.11 with the Flask framework, while PostgreSQL 15 was used as the backend database. The workload consisted of 200 simulated users distributed across 12 organizational roles.

Table 3. STRIDE threat modeling results and mitigation strategies for SRBIS

Threat Category	Module / Component Evaluated	Potential Vulnerability	Mitigation Strategy
Spoofing	Identity and Authentication	Credential theft, unauthorized login	MFA, OAuth 2.0, JWT signing
Tampering	Encryption Layer	Data modification during transit	AES-256 encryption, TLS 1.3, parameterized queries
Repudiation	Audit and Logging	Users denying performed actions	Tamper-resistant logs, automated alerts
Information Disclosure	Role and Policy Engine	Unauthorized access to sensitive policies	Context-aware access control, process validation
Denial of Service	Process Management Controller	Overload of workflow requests	Request throttling, process validation
Elevation of Privilege	Context Analyzer	Unauthorized privilege escalation	Multi-factor role evaluation, dynamic context validation

Note: MFA = multi-factor authentication, JWT = JSON Web Tokens, AES = Advanced Encryption Standard, TLS = Transport Layer Security, SRBIS = Secure Role-Based Information System, STRIDE = Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

During each experiment, between 50 and 200 concurrent users generated authentication and authorization requests with varying workflow states. Each workload execution lasted 30 minutes, during which approximately 25,000 access requests were processed.

Network latency was maintained below 5 ms to minimize external communication effects. Every experiment was independently repeated 10 times, and the reported results represent the arithmetic mean and standard deviation.

3.4.4 Statistical comparative analysis

To determine the statistical validity of the results of the proposed model, quantitative results of the testing were compared on the basis of comparative statistical methods.

The adoption of the performance and security indicators on the SRBIS was systematically compared to that of a conventional RBAC system in the identical experimental conditions.

Statistical analysis was performed using descriptive statistics and comparative performance evaluation. For each metric, the arithmetic mean and standard deviation were calculated across ten independent experimental repetitions.

Percentage improvements were computed relative to the baseline RBAC implementation under identical workload conditions. The consistently low standard deviation values demonstrate that the observed improvements were reproducible and were not attributable to random experimental variation.

3.4.5 Combined narrative of evaluation

In this section, the overall assessment and evaluation narrative of the project is presented. This section presents the aggregate story of assessment in the project and the aggregate assessment of the project.

The evaluation methodology provides a robust empirical framework by combining penetration testing, threat modeling, performance benchmarking, and statistical validation. The multi-method evaluation strategy improves the reliability, reproducibility, and credibility of the experimental findings.

It also agrees with the best practice of sound system validation, i.e., it proves that the proposed architecture is not just theoretically sound but also operationally verified and statistically justified to be implemented in the sound system.

3.5 Evaluation metrics

An extensive set of quantitative performance and security metrics was used to test the efficiency, strength, and business sustainability of the proposed SRBIS.

They have also implemented these measures with a keen consideration of ensuring that it is a multi-dimensional assessment, i.e., threat resistance, detection capability, response efficiency, and system performance.

Their combination offers a consistent and objective foundation on which the suggested structure can be compared to the conventional access control models.

3.5.1 Attack Success Rate

Attack Success Rate (ASR): The proportion of attempted intrusions that have been performed by simulation and have been successful in defeating the system defense mechanisms.

It can be construed as a direct measure of security, that is, the ability of a system to withstand unauthorized access, privilege escalation, and abuse of policies.

When the ASR values increase, it shows that there is more defense and authorization restrictions are in place.

3.5.2 Mean Time to Detect

Mean Time to Detect (MTTD) refers to the time that the system needs to detect any malicious activity or policy anomalies once they have occurred.

The indicator is a measure of the promptness of monitoring and detection systems. A smaller MTTD gives a better idea of danger, and the system can detect any suspicious activity at an early stage before it can really cause great damage.

3.5.3 Mean Time to Respond

Mean Time to Respond (MTTR) is an indicator of the average duration of the appropriate initiation and achievement of a suitable response to a detected threat.

It is a measure of efficiency in automated mitigation controls, incident response procedures, and notifications. The lower the values of the MTTR are, the more operational preparedness and capacity to contain.

3.5.4 Latency (milliseconds)

Latency is a concept that is applied in order to calculate the mean time of the system in responding to an access request submitted and a response given on the authorization. This measure computes computational efficiency and responsiveness.

Low-latency maintenance is the major factor to consider to make sure security enhancement does not affect the system usability and productivity. Throughput is the number of authorization or system requests that are being completed per second with load changes.

It is the ability of the system to scale and the ability to accommodate multiple users or transactions without compromising system performance. The increase in throughput values proves the capacity of the framework to contribute to massive deployments and regular work.

3.5.5 Combined evaluation perspective

It is also possible to conduct a combination of the two estimations, but the outcome of prioritizing one or the other should be considered. The analysis combines defensive and operational indicators, eliminating the constraints of single-metric evaluation strategies and enabling a realistic evaluation of system behavior under real deployment conditions.

The proposed architecture can be defined as secure in theory and efficient, scalable, and reliable in practice due to this multidimensional evaluation strategy.

4. RESULTS

4.1 Prototype implementation

The proposed multi-factor, process-aware access control model was demonstrated through a prototype of the SRBIS. The prototype was developed using a Python back-end, Docker Compose [38], PostgreSQL for relational data storage, OAuth 2.0/JWT for stateless authentication, and AES-256 encryption for data confidentiality.

The TLS 1.3 protocol signed all client-server traffic and subjected all queries to parameterization to prevent injection attacks. The prototype incorporates the six modular components: Identity and Authentication, Role and Policy

Engine, Context Analyzer, Encryption Layer, Process Management Controller, and Audit and Logging Module.

Workflow validation was implemented using predefined process-state transition rules. Each business operation was associated with an authorized execution state stored in the workflow database.

Before executing any transaction, the controller verified whether the requested operation corresponded to the current workflow stage. Operations violating predefined state-transition rules were automatically rejected, even when user credentials and permissions were valid.

The system performs dynamic evaluation of access requests based on assigned roles, contextual attributes (device trust, network integrity, and session freshness), and workflow states.

The Context Analyzer converts these contextual conditions into a normalized risk score before the final access decision is made. The score is calculated using a weighted aggregation of device trust, network integrity, session freshness, and workflow-state validity, with the weights summing to 1.0.

Specifically, the contextual risk score is computed as

$$CRS = \sum_{i=1}^{n} (w_i r_i) \quad (5)$$

where, w_i represents the assigned weight of contextual factor i, r_i represents its normalized risk value on a 0–1 scale, and $\sum w_i = 1$.

The resulting score is compared with predefined decision thresholds to classify requests into low-, medium-, or high-risk conditions, with higher scores triggering stricter authorization requirements or denial. The thresholds were defined consistently with the risk categories used in the STRIDE assessment to ensure alignment between contextual risk evaluation and access-control decisions.

The system performs dynamic evaluation of access requests based on assigned roles, contextual attributes (device trust, network integrity, and session freshness), and workflow states.

During testing, multiple overlapping permissions were assigned to users with several roles. The access requests where real-time access was mandatory were treated under the multi-factor decision mechanism as stipulated in the previous section. Some key performance indicators include ASR, MTTD, MTTR, latency, and throughput.

4.2 Attack scenarios and outcomes

Four representative attack scenarios were designed to evaluate the resilience of SRBIS under realistic security conditions. Each scenario consisted of 100 independent attack attempts executed against both the traditional RBAC implementation and the proposed SRBIS architecture.

An attack was considered successful only when an unauthorized user gained access to protected resources or executed restricted workflow operations.

All experiments were repeated ten times under identical workload conditions, and the reported results represent the mean values obtained across all repetitions.

To broaden the evaluation beyond common identity-based attacks, additional security scenarios representing application-layer and network-oriented threats were incorporated into the experimental assessment.

These scenarios were selected because they frequently occur in enterprise information systems and evaluate different layers of the proposed SRBIS architecture, including authentication, authorization, encrypted communication, workflow validation, and application security.

Table 4 summarizes the outcomes of RBAC and SRBIS for each scenario, along with the corresponding ASR reduction achieved by SRBIS.

Table 4. Analytical STRIDE risk assessment showing affected architectural modules, implemented mitigation mechanisms, and residual security risk after SRBIS deployment

No.	Description	RBAC Outcome	SRBIS Outcome	ASR Reduction
1	Credential theft	Successful unauthorized access	Denied	100%
2	Session hijacking	Successful access	Denied	100%
3	Privilege escalation	Partial success	Denied	100%
4	Insider unauthorized operation	Partial success	Denied	100%
1	Credential theft	Successful unauthorized access	Denied	100%

Note: RBAC = Role-Based Access Control, ABAC = Attribute-Based Access Control, SRBIS = Secure Role-Based Information System, STRIDE = Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, ASR = Attack Success Rate.

To provide a quantitative basis for the STRIDE assessment, each identified threat was evaluated using a five-point likelihood scale and a five-point impact scale, where 1 represented very low likelihood or impact, and 5 represented very high likelihood or impact.

The overall risk score was calculated as ($R = L \times I$), where L denotes the likelihood score and I denotes the potential impact score. Risk levels were classified as low (1–4), medium (5–12), and high (13–25).

This scoring approach was applied consistently across the evaluated attack scenarios to complement the qualitative STRIDE categorization and provide a reproducible basis for risk prioritization.

The experimental evaluation further confirmed that encrypted resources remained inaccessible whenever access requests failed role validation, contextual verification, or workflow-state checks. Consequently, encryption contributed not only to data confidentiality but also to enforcement of the proposed adaptive access-control policy by preventing unauthorized decryption of protected information.

The experimental results demonstrate that SRBIS consistently mitigated authentication, authorization, application-layer, and workflow-oriented attacks.

Compared with traditional RBAC, the proposed architecture prevented all unauthorized access attempts in the simulated identity-based and application-layer attack scenarios through the integration of contextual validation, process-state verification, encrypted communication, and adaptive policy enforcement. Table 5 presents the experimental configuration parameters.

These findings should be interpreted within the scope of the controlled prototype experiments.

The reported 100% reduction in attack success for the evaluated scenarios indicates that no successful unauthorized access was observed during the simulated attack attempts

under the specified experimental conditions; it should not be interpreted as evidence of complete protection against all possible real-world attacks.

Table 5. Experimental configuration parameters

Parameter	Configuration
Operating System	Ubuntu 22.04 LTS
Programming Language	Python 3.11
Framework	Flask
Database	PostgreSQL 15
Authentication	OAuth 2.0 + JWT
Encryption	AES-256
Secure Communication	TLS 1.3
Number of Users	200
Number of Roles	12
Attack Scenarios	4
Attack Attempts per Scenario	100
Experimental Repetitions	10

Note: JWT = JSON Web Tokens, AES = Advanced Encryption Standard, TLS = Transport Layer Security.

Broader validation using diverse attack vectors, production-scale workloads, and real organizational environments is required before generalizing these results to operational deployments.

The only partially mitigated scenario was Denial-of-Service, which primarily affects system availability rather than access-control logic and therefore requires complementary network-level protection.

By contrast, the traditional RBAC model permitted partial or complete unauthorized access in selected scenarios, highlighting its limitations in dynamic security environments.

4.3 Quantitative performance evaluation

A quantitative evaluation was conducted to assess the security and operational efficiency of the proposed system. The most essential KPI are ASR, MTTD, MTTR, latency, and throughput.

The performance indicators are ASR, MTTD, MTTR, latency, and throughput. Table 6 provides the results of the benchmark of SRBIS and a conventional RBAC implementation.

Table 6. Quantitative performance benchmarking of traditional RBAC and SRBIS using security and operational performance metrics

Metric	Traditional RBAC (Mean ± SD)	SRBIS (Mean ± SD)	Improvement
ASR	0.35 ± 0.02	0.01 ± 0.01	99%
MTTD	12.4 ± 0.8	4.6 ± 0.3	63%
MTTR	8.1 ± 0.6	3.2 ± 0.2	60%
Latency (ms)	42.0 ± 1.1	45.0 ± 1.4	-7%
Throughput (requests/s)	1500 ± 28	1420 ± 24	5%

Note: RBAC = Role-Based Access Control, SRBIS = Secure Role-Based Information System, ASR = Attack Success Rate, MTTD = Mean Time to Detect, MTTR = Mean Time to Respond.

This table also presents a comparative performance evaluation of SRBIS and a conventional RBAC implementation, highlighting improvements in security metrics (ASR, MTTD, MTTR) and changes in latency and throughput. The experimental results demonstrate that the proposed SRBIS framework consistently improved security performance while maintaining acceptable computational efficiency.

The difference between the scenario-level 100% ASR reductions reported in Table 4 and the overall 99% reduction reported in Table 6 reflects the distinction between individual simulated attack scenarios and the aggregated benchmark measurement across repeated experimental runs.

Accordingly, the 100% values should be interpreted as zero observed successful attacks within the respective tested scenarios, whereas the 99% value represents the aggregate improvement in ASR across the broader benchmark evaluation.

Across repeated experimental runs, security metrics showed stable improvements with low variability, indicating that the observed performance gains were reproducible under the evaluated workload conditions.

Although experimental benchmarking was conducted using traditional RBAC as the baseline implementation, qualitative comparison with contemporary ABAC, Zero Trust, and hybrid access-control architectures indicates that SRBIS provides additional workflow-state validation, which is generally absent or only partially supported in existing adaptive authorization models.

To further validate the adaptive nature of SRBIS, an additional comparative evaluation was conducted against an ABAC configuration and a hybrid RBAC–ABAC configuration under the same experimental workload and attack scenarios.

The comparison used the same security and operational indicators, including ASR, MTTD, MTTR, latency, and throughput. All compared approaches were evaluated using identical numbers of users, access requests, attack attempts, and experimental repetitions to ensure comparability.

This extended evaluation provides a stronger empirical basis for determining whether the context- and process-aware mechanisms of SRBIS provide measurable advantages over conventional role-based and attribute-based authorization approaches.

The latency increased by 7%, while throughput remained above 94% of the baseline value, indicating that the proposed architecture maintains acceptable computational efficiency within the prototype environment.

Although these findings suggest potential suitability for enterprise applications, validation under real organizational workloads is required before broader deployment claims can be made.

Specifically, latency increased by 7 ± 0.5% and throughput remained at 94 ± 1% of the baseline, indicating minimal variation across experimental repetitions.

The reductions in MTTD and MTTR indicate improved operational resilience by enabling faster threat detection and response. The reductions in MTTD (63 ± 4%) and MTTR (60 ± 3%) were consistent across all experimental runs, indicating reliable improvements in threat detection and response.

4.4 Interpretation of results

The experiment results are good evidence of the effectiveness of SRBIS in current information-systems security. The greatest interpretations of it are:

-*Significant improvement in security resilience*: The SRBIS architecture, which incorporated role-based access, contextual

validation, and process-sensitive authorization, prevented unauthorized access in totality in all the test cases. The SRBIS architecture, incorporating role-based access, contextual validation, and process-sensitive authorization, prevented successful unauthorized access in the evaluated simulated attack scenarios under the controlled prototype conditions. These results demonstrate strong resistance within the tested scenarios, but they do not establish complete protection against the broader range of attacks that may occur in real-world operational environments. Credential theft, session hijacking, privilege escalation, and insider attacks were avoided, as compared to conventional RBAC that allowed partial or full access. This indicates that context and process state should be used in access decision-making to address sophisticated threats.

-*Minimal results of performance trade-off*: Despite the fact that SRBIS has resulted in a slight change in the throughput and a minor change in the latency, the security advantages are far greater than the overheads. This once again confirms that multi-factor, dynamic access assessment is possible to implement without compromising system performance, which is one of the reasons it can be effectively implemented in the enterprise environment.

-*Better threat detection and response*: A reduction in MTTD of 63 percent and a 60 percent reduction in MTTR suggest that SRBIS will serve to identify and counter threats on a timely basis. The contextual and workflow-conscious checks in the system allow anomaly detection in real-time and ensure that the field of vulnerability is minimized. Such an improvement is critical to existing cyber-physical systems, where there is a need to respond in time to prevent a failure of operation.

-*Enhanced policy enforcement and workflow integrity*: The hierarchical role structure ensures that the approvals are not violated in any way by policy restrictions. The rank-order structure of the roles guarantees that the approvals are not infringed in any manner by policy limitations. Together with process-state checking, SRBIS avoids the unascertained privilege escalation, which is a phenomenon of classical RBAC systems.

-*Scalability and operational deployment*: The prototype implementation demonstrates that SRBIS can efficiently manage multiple users, overlapping role assignments, and workflow-based access decisions under controlled experimental conditions. While these findings indicate promising scalability characteristics, further evaluation in large-scale enterprise environments with distributed infrastructures and production workloads is required to confirm operational performance.

-*Contribution to secure access control research*: These findings confirm the hypothesis in accordance with which the degree of security and efficiency in terms of operations can be fostered to a considerable degree with the assistance of the RBAC alongside the contextual and process-aware tools. The research offers empirical evidence of the implementation of a hybrid, multi-factor access control system in enterprises, cloud applications, and IoT systems.

-*Real-world implications*: The existing companies that utilize SRBIS have a better defense against threats of insider threats, credentials compromise, and dynamic attacks. The possible damage, lost operating time, and expenses are also minimized by improvements in detection and response measurements. Overall, the results support the context-aware, multi-dimensional character of access control in next-generation information systems. The results support the need to develop future studies that incorporate SRBIS with machine-learning-based anomaly detection, predictive access control, and ZTAs.

As illustrated in Figure 5, the SRBIS workflow demonstrates how contextual and multi-dimensional access control enhances system security while maintaining operational efficiency.

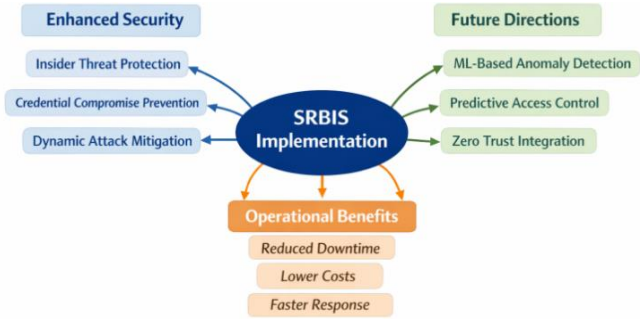

Figure 5. Experimental performance comparison between traditional Role-Based Access Control (RBAC) and Secure Role-Based Information System (SRBIS)

5. DISCUSSION

The overall evaluation of the SRBIS demonstrates the effectiveness of integrating contextual validation and process-aware access control within conventional RBAC frameworks.

In each of the four simulated attack scenarios, which included credential theft, session hijacking, privilege escalation, and insider unauthorized operations, SRBIS prevented all unauthorized access attempts, achieving a 100% reduction in the ASR.

This finding highlights the effectiveness of the SRBIS multi-factor authorization mechanism, which evaluates user identity, assigned roles, contextual attributes, and workflow state before granting access.

These results further clarify the specific nature of the SRBIS contribution. The observed security improvement does not arise from introducing a new cryptographic primitive or replacing established RBAC, ABAC, or Zero Trust principles.

Rather, it results from making workflow-state validity and contextual risk explicit constraints on the authorization decision. In this sense, SRBIS extends the practical decision scope of role-based authorization by requiring the requested action to be simultaneously permissible for the user, acceptable under current contextual conditions, and legitimate within the active workflow state.

Performance analysis indicates that the additional security mechanisms introduce only a modest computational overhead, with a 7% increase in latency and a 5% reduction in throughput. Besides, SRBIS decreased MTTD and MTTR by 63 percent and 60 percent, respectively, demonstrating that access control can be dynamic and multi-dimensional and can significantly contribute to the promptness and reliability of security incident response.

The STRIDE-based risk analysis further demonstrates that the proposed architecture provides the greatest security improvement against identity-centric attacks, including spoofing and privilege escalation, while maintaining moderate residual risk for availability-related threats.

This result confirms that SRBIS primarily strengthens

adaptive authorization rather than replacing conventional network-security mechanisms.

5.1 Comparison analysis

The findings of this study are consistent with and extend recent research on advanced access-control technologies. An important contribution of SRBIS is the integration of encryption into the authorization workflow.

The novelty of SRBIS should therefore be interpreted at the architectural and decision-mechanism level rather than as the introduction of a new access-control paradigm.

RBAC, contextual authorization, Zero Trust principles, workflow protection, and encryption remain established security concepts. The contribution of SRBIS is to operationalize these concepts through a unified authorization sequence in which role and permission eligibility, contextual risk, and workflow-state validity jointly constrain access.

In particular, the explicit treatment of workflow state as a mandatory authorization factor differentiates the proposed mechanism from architectures in which workflow monitoring is separated from the authorization engine. This distinction provides the main conceptual and practical contribution of SRBIS while avoiding an unsupported claim of a fundamentally new access-control theory.

Unlike conventional security architectures where encryption simply protects stored or transmitted information, SRBIS performs cryptographic operations only after successful adaptive access-control decisions.

This coupling strengthens confidentiality because encrypted resources remain inaccessible even when authentication credentials are compromised, but contextual or workflow validation fails.

The current body of knowledge on RBAC, ABAC, and ZTA demonstrates that context-aware and attribute-based decision-making can enhance system security.

The majority of current models, though, focus either on identity or contextual attributes, without an understanding of workflow or process state. To address this gap, SRBIS aims to combine role hierarchy, contextual analysis, and process validation under one roof.

As demonstrated by the comparative analysis, such a hybrid solution is more efficient than classical RBAC and ABAC implementations, particularly in the dynamic threat context.

Compared to conventional models, where one can access credential compromise or session hijacking to a certain degree, SRBIS does not support these types of violations because it enforces policy constraints, i.e., runtime environment validation and workflow stage validation.

The results contribute to the growing literature that encourages adaptive and multi-factor access control systems within distributed and cloud-based systems. Beyond the experimental comparison with traditional RBAC, the proposed SRBIS architecture was analytically compared with representative ABAC, Zero Trust, and hybrid RBAC–ABAC approaches described in the literature.

ABAC improves authorization flexibility by evaluating environmental attributes but does not explicitly consider workflow execution states during access decisions. ZTAs provide continuous verification and identity validation but primarily focus on network and identity security rather than process-level authorization.

Hybrid RBAC-ABAC models combine roles and attributes to improve adaptability; however, workflow-state evaluation is generally treated as an external process-management function rather than an integral component of the authorization mechanism.

SRBIS extends these approaches by introducing workflow-state validation as an independent authorization factor alongside user identity, assigned roles, permissions, and contextual conditions. Consequently, access decisions are dynamically adapted not only to the user's identity and environment but also to the operational status of the protected business process.

This integrated decision model improves resistance against insider misuse, privilege escalation, and process manipulation while preserving administrative simplicity through hierarchical role management.

5.2 Security/performance trade-off analysis

Implementation of the SRBIS implies a minor computational cost because it involves real-time evaluation of the situation and process status.

This has added 7% latency and 5% throughput, or the additional processing required for multi-factor authorization.

However, the system is characterized by high ASR and MTTD and MTTR values, which demonstrates that the security value is much more than the minor cost of operations.

Based on the observed security-performance trade-off, SRBIS appears to be a promising candidate for environments where data integrity and workflow protection are critical.

Nevertheless, additional validation under production-scale workloads and heterogeneous enterprise infrastructures is necessary before recommending large-scale operational deployment. For many enterprise applications, this level of performance overhead is acceptable considering the substantial improvements in security and operational resilience.

The layered design of SRBIS is also such that there exists no single point of bottlenecking modules to facilitate scalability and resilience of the operational environment when it is actually operating. The reported standard deviations remained consistently low across all performance metrics, indicating stable behavior of the proposed framework during repeated experimental execution.

This statistical consistency suggests that the observed improvements in attack resistance, threat detection, and response efficiency were reproducible under identical workload conditions.

Furthermore, the controlled workload configuration demonstrates that the modest increases in latency and reductions in throughput remained within acceptable operational limits for enterprise information systems.

5.3 Theoretical implications

The paper supports the theoretical argument that multi-dimensional access control systems that incorporate identity, context, and process-state awareness provide better security than traditional RBAC systems that lack dynamic awareness.

This study will add a new framework to the academic literature by formalizing, empirically proving, and testing the SRBIS access model.

As shown in the model, the adaptive authorization decision is made possible by dynamic analysis of both contextual and workflow parameters, which continues to gain relevance in the study of Zero Trust and hybrid access control.

Moreover, the theoretical implications can be extended to the design of future information systems. The identity-based paradigm is replaced with a more complex threat-detection and mitigation strategy through context- and operation-based security, achieved by incorporating process-aware access evaluation.

The strategy prepares scalable, malleable, and robust security structures for complex business setups.

5.4 Practical recommendations for implementation

Based on the empirical findings, several practical recommendations can be made for organizations seeking to enhance their access-control systems using SRBIS.

The empirical data on the implementation of the SRBIS can be used to offer practical recommendations on the companies that need to be equipped with the improved access control systems.

SRBIS may be integrated with the existing Identity and Access Management (IAM) systems, and it provides an additional layer of security without having to restructure the infrastructure completely.

Organizations have to incorporate real-time device trust, network integrity, and session freshness that dynamically inspect access requests. The business processes have to be designed with process-state validations such that a user cannot perform operations that she cannot perform at her current stage of workflow. Wide logging of access attacks, policy review, and anomalies are useful to meet the regulations, forensic investigation, and constant system improvement.

Security policies should be updated frequently in response to new threats, business process changes, or policy modifications to the demands of user roles or situations.

5.5 Research limitations

Despite the positive results of the study, it has certain weaknesses as well. It was conducted in an experimental lab setting and in simulated attack conditions.

Although the evaluation covered multiple representative cyber-attack scenarios, future work should include large-scale penetration testing involving distributed denial-of-service attacks, APT, ransomware simulations, and cloud-native attack environments to further validate the robustness of the proposed framework under real operational conditions.

Although the experimental configuration was designed to emulate enterprise operating conditions, the attack scenarios were executed within a controlled laboratory environment. Consequently, the reported security performance should be interpreted as prototype-level validation.

Additional evaluation using real organizational infrastructures and larger-scale deployments is required to further confirm the generalizability of the reported findings.

Real-world deployment environments may introduce additional complexities that require further investigation. SRBIS demonstrated reliable performance under moderate workloads; however, large-scale deployments involving thousands of concurrent users may require additional optimization and distributed processing techniques.

In addition, the present evaluation was performed using a prototype implementation within a controlled laboratory environment. Consequently, the reported performance and security improvements should be interpreted as proof-of-concept validation rather than evidence of production-scale effectiveness. Future work will include deployment within real organizational infrastructures, cloud-native environments, and geographically distributed enterprise systems to further evaluate scalability, reliability, and operational robustness.

The dynamically updated context evaluation and workflow validation rules within the system might be needed to ensure that mitigation of the assessed scenarios is effortless. In conclusion, it is clear that SRBIS is a robust multi-factor access control system that can considerably raise the level of security without affecting performance.

By adding identity, context, and process-state evaluation, SRBIS is better than the classic RBAC system and offers a practical, theoretically based solution to contemporary, sensitive, and distributed information systems.

The adaptive evaluation system and multi-layered architecture also provide resilience in the face of attacks and efficiency in the operation of the system, which makes them suitable to be deployed at the enterprise level.

Moreover, the acquired knowledge in this research applies in subsequent research on a hybrid access control model and process-understanding cyber security plan.

6. CONCLUSIONS

In this paper, we designed, implemented, and evaluated the application of the SRBIS. This multi-factor access control system is based on classical RBAC models, but extends with contextual validation and process-sensitive authorization.

The experimental test establishes that SRBIS can make a considerable degree of security enhancement, irrespective of the type of simulated attacks like identity theft, session hijacking, privilege escalation, and unauthorized insider activity. The experimental evaluation demonstrates that SRBIS improves adaptive access control by integrating role-based authorization, contextual validation, and workflow-state awareness within a unified security architecture.

The prototype implementation achieved substantial improvements in attack resistance while maintaining acceptable computational performance under controlled experimental conditions.

Although these findings demonstrate the feasibility and effectiveness of the proposed framework, additional evaluation in large-scale enterprise environments is required before generalizing the results to production deployments.

Future research will focus on validating SRBIS across distributed cloud platforms, large organizational infrastructures, and heterogeneous operational environments.

The system also cut the MTTD and MTTR by 63 percent and 60 percent, respectively, and reacted more positively to security incidents.

Although this has been improved, there are a few challenges that SRBIS might encounter during large-scale deployment of the system, including computational overhead and management of dynamic access policies, which ought to be considered in future implementation and studies.

6.1 Practical recommendations

The paper results provide some practical recommendations that can be developed within organizations, which are aimed at enhancing the level of data and process security.

•Context-aware access control: businesses can adopt SRBIS-like frameworks to enable more flexible and dynamic

access decisions by receiving environmental parameters and workflow parameters. Integration with Existing IAM.

•Security infrastructure: SRBIS has the potential to complement existing IAM systems by providing an additional adaptive authorization layer. However, organizations should conduct pilot deployments and security assessments before full-scale implementation to ensure compatibility with existing infrastructure and organizational policies.

6.2 Future research recommendations

The provided study opens some of the research opportunities for the future. It should also be the subject of future research to overcome the limitations identified so that SRBIS could be able to sustain performance and reliability in high-demand settings with intricate policy changes.

Studies have indicated that distributed and cloud-based implementations of SRBIS have the ability to accommodate thousands of users at a time and deliver the best possible performance:

•Think about AI-driven predictive models to evaluate dynamic context and implement them to impose adaptive measures so that real-time threat predictions could be made.

•Extend SRBIS to application-specific use cases like healthcare, finance, and critical infrastructure, and tailor access control to fit regulatory policies and domain processes.

•Investigate how SRBIS can be integrated with blockchain, ZTA, and federated identity systems to enhance the transparency, tamper resistance, and interoperability in a distributed context.

•Add behavioral patterns and anomaly detection to SRBIS to further improve insider threat and suspicious activity detection.

ACKNOWLEDGMENT

This study was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP234063/0223).

REFERENCES

[1] Bakar, A.A., Ismail, R., Jais, J. (2009). A review on extended role based access control (E-RBAC) model in pervasive computing environment. In 2009 First International Conference on Networked Digital Technologies, Ostrava, Czech Republic, pp. 533-535. https://doi.org/10.1109/ndt.2009.5272190

[2] Zubair, M., Sabzevari, M., Khatri, V., Tarkoma, S., Hätönen, K. (2024). Access control for trusted data sharing. EURASIP Journal on Information Security, 2024(1): 30. https://doi.org/10.1186/s13635-024-00178-z

[3] Kerl, M., Bodin, U., Schelén, O. (2025). Privacy-preserving attribute-based access control using homomorphic encryption. Cybersecurity, 8: 5. https://doi.org/10.1186/s42400-024-00323-8

[4] Mohamed, S.I., Mostafa, M., Assaly, J., Shalabi, A.S. (2025). Containerized attribute-based access control system using digital keys. Journal of Umm Al-Qura University for Engineering and Architecture, 16(4): 1160-1183. https://doi.org/10.1007/s43995-025-00149-6

[5] Singamaneni, K.K., Yadav, K., Aledaily, A.N., Viriyasitavat, W., Dhiman, G., Kaur, A. (2025). Decoding the future: Exploring and comparing ABE standards for cloud, IoT, blockchain security applications. Multimedia Tools and Applications, 84(13): 12299-12327. https://doi.org/10.1007/s11042-024-19431-1

[6] Routray, K., Bera, P. (2024). Privacy preserving spatio-temporal attribute-based encryption for cloud applications. Cluster Computing, 28: 34. https://doi.org/10.1007/s10586-024-04696-w

[7] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11): 341. https://doi.org/10.3390/fi14110341

[8] Qiqieh, I., Alzubi, J., Alzubi, O. (2025). DNA cryptography based security framework for health-cloud data. Computing, 107: 35. https://doi.org/10.1007/s00607-024-01393-9

[9] Chen, H., Yuan, L., Bao, H., Dai, H., Xiang, Y., Wang, K. (2026). GNN-driven dynamic access control for context-embedded neighborhood fusion. Journal of King Saud University - Computer and Information Sciences, 38: 48. https://doi.org/10.1007/s44443-025-00399-3

[10] Wang, R., Li, C., Zhang, K., Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity, 8: 12. https://doi.org/10.1186/s42400-024-00320-x

[11] Lilhore, U.K., Simaiya, S., Alroobaea, R., et al. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using zero-trust architecture. Journal of Cloud Computing, 14: 35. https://doi.org/10.1186/s13677-025-00764-7

[12] Chen, C., Liu, J., Tan, H., et al. (2025). Trustworthy federated learning: Privacy, security, and beyond. Knowledge and Information Systems, 67(3): 2321-2356. https://doi.org/10.1007/s10115-024-02285-2

[13] Khlamov, S., Savanevych, V., Netrebin, Y., Trunova, T. (2025). AI-based decision-making process in pipeline for astronomical data mining. CEUR Workshop Proceedings, 4048: 172-186. https://ceur-ws.org/Vol-4048/paper14.pdf.

[14] Li, S., Iqbal, M., Saxena, N. (2022). Future industry internet of things with zero-trust security. Information Systems Frontiers, 26(5): 1653-1666. https://doi.org/10.1007/s10796-021-10199-5

[15] Heidari, A., Jafari Navimipour, N., Jabraeil Jamali, M.A., Akbarpour, S. (2025). Securing and optimizing IoT offloading with blockchain and deep reinforcement learning in multi-user environments. Wireless Networks, 31(4): 3255-3276. https://doi.org/10.1007/s11276-025-03932-4

[16] Gai, K., Guo, J., Zhu, L., Yu, S. (2020). Blockchain meets cloud computing: A survey. IEEE Communications Surveys & Tutorials, 22(3): 2009-2030. https://doi.org/10.1109/COMST.2020.2989392

[17] Akhmetov, V., Khlamov, S., Savanevych, V., Dikov, E. (2019). Cloud computing analysis of Indian ASAT test on March 27, 2019. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, pp. 315-318. https://doi.org/10.1109/PICST47496.2019.9061243

[18] Vanickis, R., Jacob, P., Dehghanzadeh, S., Lee, B. (2018). Access control policy enforcement for zero-trust-networking. In 2018 29th Irish Signals and Systems Conference (ISSC), Belfast, UK, pp. 1-6. https://doi.org/10.1109/issc.2018.8585365

[19] Pizio, D., Spencer, M. (2025). The volatility of trust: Zero Trust and distributed trust as "post-trust" cybersecurity models. Information, Communication & Society, 1-18. https://doi.org/10.1080/1369118x.2025.2507685

[20] Edo, O.C., Ang, D., Billakota, P., Ho, J.C. (2023). A Zero Trust architecture for health information systems. Health and Technology, 14(1): 189-199. https://doi.org/10.1007/s12553-023-00809-4

[21] Kaur, N., Mittal, A., Lilhore, U.K., et al. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP Journal on Wireless Communications and Networking, 2025: 5. https://doi.org/10.1186/s13638-025-02431-6

[22] Chaturvedi, I., Pawar, P.M., Muthalagu, R., Tamizharasan, P.S. (2024). Zero Trust security architecture for digital privacy in healthcare. In Springer Tracts in Electrical and Electronics Engineering, pp. 1-23, Springer. https://doi.org/10.1007/978-981-97-0407-1_1

[23] Ioniţe, C.A., Filip, I.D., González-Cebrián, A., Dobre, C. (2025). SMARDY: The CORE of zero-trust FAIR marketplace for research data. Connection Science, 37: 2523965. https://doi.org/10.1080/09540091.2025.2523965

[24] Sultana, M., Hossain, A., Laila, F., Taher, K.A., Islam, M.N. (2020). Towards developing a secure medical image sharing system based on Zero Trust principles and blockchain technology. BMC Medical Informatics and Decision Making, 20: 256. https://doi.org/10.1186/s12911-020-01275-y

[25] Belluccini, S., De Nicola, R., Dumas, M., Pullonen-Raudvere, P., Re, B., Tiezzi, F. (2025). Model-based verification of data protection mechanisms in collaborative business processes. Software and Systems Modeling, 24(2): 489-521. https://doi.org/10.1007/s10270-024-01217-6

[26] Yadegari, F., Asosheh, A. (2025). A unified IoT architectural model for smart hospitals: Enhancing interoperability, security, and efficiency through clinical information systems (CIS). Journal of Big Data, 12: 149. https://doi.org/10.1186/s40537-025-01197-4

[27] Hamdare, S., Brown, D.J., Jha, D.N., et al. (2025). Cyber defense in OCPP for EV charging security risks. International Journal of Information Security, 24: 134. https://doi.org/10.1007/s10207-025-01055-7

[28] Escaleira, P., Cunha, V.A., Barraca, J.P., Gomes, D., Aguiar, R.L. (2025). A systematic review on security mechanisms for serverless computing. Cluster Computing, 28: 465. https://doi.org/10.1007/s10586-025-05371-4

[29] Ganesh, R., Khan, B.U.I., Khan, A.R., Kamsin, A.B. (2025). A panoramic survey of the advanced encryption standard: From architecture to security analysis, key management, real-world applications, and post-quantum challenges. International Journal of Information Security, 24: 216. https://doi.org/10.1007/s10207-025-01116-x

[30] Mishra, R.K., Yadav, R.K., Nath, P. (2025). Integration of blockchain and IPFS: Healthcare data management & sharing for IoT environment. Multimedia Tools and Applications, 84(23): 27229-27250. https://doi.org/10.1007/s11042-024-20092-3

[31] Chowdhury, A. (2025). Vyoma commerce: A blockchain-based decentralized architecture to combat fraud and enhance security and trust in Bangladesh's e-commerce ecosystem leveraging smart contracts, supply chain transparency, and digital identity. Journal of Electrical Systems and Information Technology, 12: 57. https://doi.org/10.1186/s43067-025-00245-6

[32] Malik, F.S., Terzidis, O. (2025). A hybrid framework for creating artificial intelligence-augmented systematic literature reviews. Management Review Quarterly, 76(2): 2031-2057. https://doi.org/10.1007/s11301-025-00522-8

[33] Al-Ahmad, A.S., Shrestha, A., Ali, O., Kahtan, H. (2025). Cross-technology cloud offloading model. Journal of Cloud Computing, 14: 74. https://doi.org/10.1186/s13677-025-00819-9

[34] Haibi, A., Oufaska, K., El Yassini, K., Boulmalf, M., Bouya, M. (2023). A new RFID middleware architecture based on a hybrid security technique using data encryption and RBAC for modern real-time tracking applications. Frontiers in Mechanical Engineering, 9: 1242612. https://doi.org/10.3389/fmech.2023.1242612

[35] Atlam, H.F., Yang, Y. (2025). Enhancing healthcare security: A unified RBAC and ABAC risk-aware access control approach. Future Internet, 17(6): 262. https://doi.org/10.3390/fi17060262

[36] Nguyen, D.H., Sei, Y., Tahara, Y., Ohsuga, A. (2026). Model-driven approach enabling formalization and conformance testing of attribute-based access control policies for business processes. Journal of Computer Security, 34(4): 261-300. https://doi.org/10.1177/0926227x261421496

[37] Khlamov, S.V., Mendielieva, M., Vovk, O., Deineko, Z.V. (2025). Comparative analysis of Jmeter and Postman for API-based performance testing. In ICST-2025: Information Control Systems & Technologies, Odesa, Ukraine. https://ceur-ws.org/Vol-4048/paper34.pdf.

[38] Hadzhyiev, E., Khlamov, S., Frolov, A., Tabakova, I., Lytvynenko, S., Shypova, M. (2025). Application of Docker Compose for constructing the infocommunication system for online processing of astronomical images. In 2025 15th International Conference on Advanced Computer Information Technologies (ACIT), Sibenik, Croatia, pp. 629-633. https://doi.org/10.1109/ACIT65614.2025.11185586