Data Privacy Protection and Access Control Mechanisms in Cross-Domain Cloud Computing Environments

Hao Lu[1,*], Peng Zhu[1] and Lifeng Liu[2]

[1]*Department of Software Engineering, Jiangxi Vocational & Technical College of Information Application, Nan chang 330000, Jiangxi, China*
[2]*Adult Education Centre, Jiangxi Vocational & Technical College of Information Application, Nan chang 330000, Jiangxi, China*
E-mail: haoluhl@outlook.com
[*]*Corresponding Author*

Received 09 July 2025; Accepted 02 December 2025

Abstract

This article offers multi-domain privacy and access control. For safe and flexible resource access, we recommend trust mechanisms, RBAC, and ATBAC. The differentiated privacy techniques in our design protect sensitive data. We build classes and connections that represent access control and privacy protection's complexity to support our suggested system's implementation and assessment. Access Control Match Score, Privacy Constraint Score, Cross-Domain Enforcement Rate, and User-Role-Resource Graph Density have positives and downsides, according to our study. The proposed system excels in policy enforcement, trust, and privacy with a dense role-resource structure, optimal privacy, best access match, and robust cross-domain enforcement. Access rates and trust levels and how privacy noise affects query results are also presented. Experimental findings show that the suggested model outperforms others. Over the best baseline, it increases ABAC match success

Journal of Cyber Security and Mobility, Vol. 14_6, 1447–1474.
doi: 10.13052/jcsm2245-1439.1466

by 18.5%, RBAC approval rate by 17.1%, and access throughput by 13.6%. It also reduces differential privacy noise by 20%, improving the privacy-utility tradeoff, and has a good connection (0.87) between trust measures and access choices.

Keywords: Data privacy protection, access control mechanisms, cross-domain cloud computing, cloud security, attribute-based access control (ABAC), role-based access control (RBAC), differential privacy and trust management.

1 Introduction

Conventional cloud computing networks are becoming steadily more evident as a result of the growing need for Internet of Things devices [1]. The disadvantages of cloud computing are eliminated by the new computing paradigm known as edge computing [2]. When application service computation and storage are moved to the network edge, this is known as edge computing. This results in the migration of attack risks to the edge of the network. Security approaches that are cloud-centric are not effective for distributed security [3]. In order to ensure the safety of the edge, researchers have implemented authentication and privacy protection measures [4]. Nevertheless, regular interactions have the potential to compromise or "mutiny" nodes into ones that are malicious. As a result of faulty nodes communicating inaccurate computations to spoof, calculation validity is compromised to varying degrees [5].

The security of blockchain technology promises to meet the expectations for trust. The basic problems associated with edge computing, such as privacy and data security, are resolved by this method [6–8]. Blockchain and distributed ledger technologies (DLTs) improve cross-domain access control trust and accountability. Blockchain provides an immutable, tamper-evident audit layer for policy modifications, trust scores, and access choices across domains in multi-domain environments with various administrative authorities. This decentralized consensus strengthens transparency and non-repudiation by preventing any domain from manipulating access records or trust declarations. Smart contracts automate RBAC/ABAC rule enforcement, assure policy interpretation, and enable dynamic trust negotiation without a central authority. Thus, adding DLTs to our system would enhance the trust-RBAC-ABAC architecture by enabling access event provenance, cross-domain policy synchronization, and auditable compliance trails.

Blockchain-enabled access governance may improve trust, accountability, and interoperability, especially in federated contexts where autonomous domains must work securely.

Individual nodes accentuate the conflicting high consensus consumption and slow pace, which limits their performance [9]. Their high consensus speed assures that blockchain applications are of good quality. Research on combining blockchain with edge computing has emerged [10, 11] as a result of the addition of blockchain services such as networking, storage, and computation for both the core and edge computing capability levels. Communication entities that are already in existence for SE solutions share an environment. The user implementation of search functionalities in contexts with many domains is not taken into consideration [12]. Ciphertext is stored and searched on separate servers, which strikes a balance between efficiency and functionality [13]. On the other hand, there are still problems with server access control and secure interaction.

The capabilities of network storage are vastly improved by cloud computing because it enables on-demand access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services). These resources are made available for rapid provisioning and release with minimal management effort or interaction with service providers [14–16]. In the event that a company that uses the cloud to store electronic information becomes involved in an investigation or lawsuit, the company is required to take into consideration the applicable laws before commencing the process of gathering, evaluating, and creating electronic data that is responsive [17–20].

The vast majority of data privacy and protection legislation safeguard the individually identifiable information of the residents of each nation. These rules, in general, control the right of entities and individuals to "process" – that is, collect, maintain, organize, store, use, and so on – the data of other individuals, and they apply whenever someone stores, gathers, processes, or sends information to or from the nation [21–24].

To guarantee the integrity and secrecy of outsourced data [25], a secure and effective outsourced computation system is provided for privacy computing. This method is suitable in cases where data privacy is valued. Blockchain with attribute-based encryption (ABE) [26] offers a fast and privacy-preserving energy trade solution for smart grids. The application protects user identities and energy consumption patterns and assures safe and confidential energy trading. Underlining the requirement of robust security mechanisms to safeguard edge devices and data, an overview of security

processes in edge computing environments is presented [27–29]. The work offers a fresh searchable encryption technique guaranteeing query performance and data confidentiality. For safe distributed cloud storage guaranteeing data confidentiality and query performance, a multi-server searchable data encryption approach is proposed [30]. The approach guarantees data privacy and integrity by enabling secure data interchange and retrieval across many servers. Presented is an attribute-based access control architecture for smart cities that allows secure data interchange and fine-grained access control using smart contracts [31]. The structure guarantees effective and safe access control, therefore protecting private information and preventing illegal access. Developed is a situation-aware system for efficient device authentication in smart grid-enabled home area networks, therefore enhancing security and reducing authentication overhead [32]. The method ensures safe device authentication, protections against probable security issues, and improves network performance.

Access control and auditing in cloud systems may be accomplished in several ways. Fundamentally, Method A, Role-Based Access Control (RBAC) [33] is a means of restricting system access to authorised individuals according on their responsibilities. Though widely used in commercial and cloud applications, RBAC is not well suited for fine-grained or context-aware access. Attribute-Based Access Control (ABAC) Method B [34] is a complex paradigm extending RBAC to support multi-domain and multi-policy contexts. By use of user, resource, and environmental traits, ABAC offers fine-grained control. In order to reconcile privacy protection with system openness, Method C, Differential Privacy-Based Access Auditing [35], details an auditing approach for data access in clouds. Each of these approaches offers many means to access auditing and control, with advantages and drawbacks.

Machine learning and AI techniques further enhance our framework by enabling adaptive, context-aware decision-making across domains. AI-driven behavioral modeling, trust prediction, and anomaly detection allow the system to dynamically adjust RBAC/ABAC rules, refine trust scores, and anticipate access risks. This leads to more accurate match scoring, improved cross-domain policy enforcement, and faster response to evolving access conditions.

In our framework, machine learning components are integrated to support adaptive access control decisions across domains. Behavioral analytics models estimate trust scores and identify anomalous access attempts, while reinforcement learning modules adjust RBAC/ABAC parameters based on

historical outcomes and policy constraints. A graph-based learner processes the user–role–resource topology to optimize match scoring and predict cross-domain access conflicts. These AI-driven modules operate in tandem with the trust engine and privacy layer, enabling dynamic, context-sensitive enforcement.

1.1 Contribution

A fully integrated, multi-layer architecture that blends access control, trust management, privacy preservation, and machine intelligence across domains advances hybrid RBAC–ABAC systems beyond static, rule-driven role and attribute combinations. The proposed system uses cross-domain trust inference and a unified user–role–resource graph structure to harmonize role hierarchies and attribute meanings across companies, unlike previous models that operate inside a single administrative boundary. Directly integrating differential privacy into the authorization process allows trust levels, data sensitivity, and domain origin to adaptively manage privacy noise and quantify DP budget utilization with a unique privacy constraint score. Dynamic, context-aware authorization is achieved via machine learning–driven adaptive policy matching employing attribute prediction, trust regression models, and graph-based policy pruning. By cryptographically confirming access rather than logical approvals, proxy re-encryption and federated key management at the enforcement layer ensure cross-domain data transfer. The study assesses these capabilities using four composite measures: Access Control Match Score, Privacy Constraint Score, Cross-Domain Enforcement Rate, and User–Role–Resource Graph Density. The metrics address structural and privacy vulnerabilities missed in hybrid RBAC–A. With 18.5% ABAC match accuracy, 17.1% RBAC approval rate, 13.6% throughput increase, 20% differential privacy noise reduction, and a strong 0.87 trust–decision correlation, the technique improves performance rather than conceptual integration. This paper presents a multi-domain, privacy-aware, ML-augmented, cryptographically enforced, empirically validated access control framework with higher flexibility, interoperability, and decision quality than hybrid RBAC–ABAC literature.

2 Proposed Model

In order to provide a complete framework for access control and privacy preservation in multi-domain contexts, the proposed model theory combines

trust mechanisms with differential privacy preservation, Attribute-Based Access Control (ABAC), and Role-Based Access Control (RBAC). It covers fundamental components including domains with unique identities and trust levels, users defined by attributes and roles, resources defined by attributes, trust relationships among domains, access control mechanisms that ascertain user privileges, and differential privacy mechanisms protecting sensitive data by introducing noise to query outputs, so providing a flexible and scalable solution for access control and privacy preservation. Development of access control rules based on ABAC and RBAC results in a system model including many domains, users, resources, and activities. RBAC users are assigned roles and rights that specify what activities they might be allowed on resources. On the other hand, ABAC grants access based on user and resource conditions, therefore allowing fine-grained control.

The proposed model consists of:

- Access control policies (ABAC, RBAC)
- Privacy constraints (differential privacy, encryption)
- Cross-domain policy enforcement
- User-role-resource relationships

2.1 System Model Definition

Let the cloud environment consist of multiple domains:

- Let $D = \{d_1, d_2, \ldots, d_m\}$, be the set of cloud **domains**, $U = \{u_1, u_2, \ldots, u_n\}$ be the set of **users**, $R = \{r_1, r_2, \ldots, r_k\}$ be the set of **resources** and $A = \{a_1, a_2, \ldots, a_l\}$ be the set of **actions** (e.g., read, write, delete)

2.2 Access Control Policy Model

(a) Role-Based Access Control (RBAC)
RBAC is a widely used access control mechanism that grants access to resources based on a user's role within an organization. In RBAC, roles are defined based on the user's job function, department, or other characteristics.

- Role Assignment:
  $RA \subseteq U \times \mathcal{R}$, where $\mathcal{R}$ is the set of roles. This relation specifies which users are assigned to which roles.
- Permission Assignment:
  $PA \subseteq \mathcal{R} \times (A \times R)$ relation specifies which permissions are assigned to which roles. Permissions are typically defined as a pair

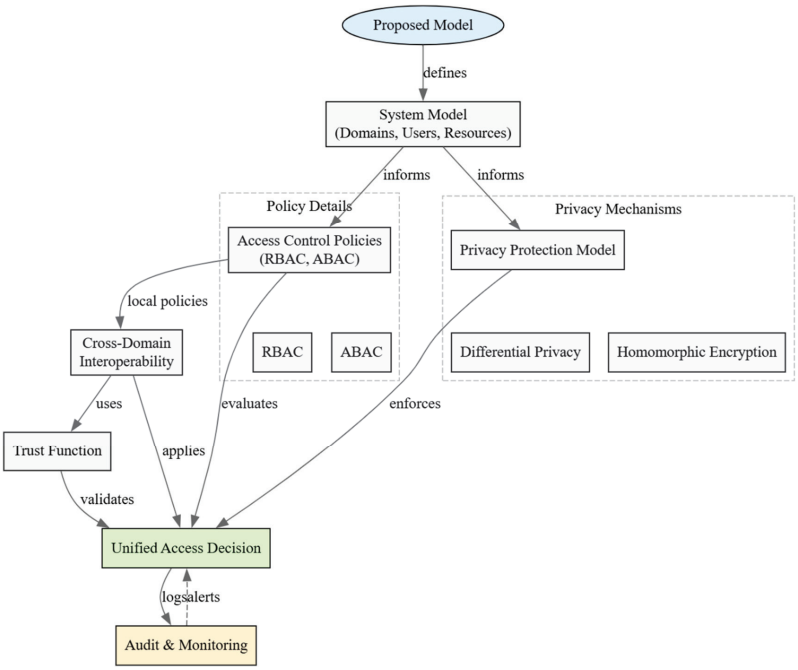


Figure 1 Block diagram for proposed model.

(action, resource), where action is the operation being performed (e.g., read, write, delete) and resource is the object being accessed. A user $u \in U$ is allowed to perform action $a \in A$ on resource $r \in R$ if:

$$\exists \rho \in \mathcal{R} : (u, \rho) \in RA \wedge (\rho, (a, r)) \in PA$$

A user can access a resource if they are assigned to a role that has the necessary permissions to perform the desired action on that resource.

(b) Attribute-Based Access Control (ABAC)
ABAC is a more fine-grained access control mechanism that grants access to resources based on a user's attributes and the attributes of the resource being accessed. Let us assume,

- $attr_u(u) \rightarrow$ set of user attributes
- $attr_r(r) \rightarrow$ set of resource attributes
- P be a set of attribute-based policies

Each policy $p \in P$ is a predicate over these attributes:

$$p : attr_u(u), attr_r(r) \Rightarrow \{allow, deny\}$$

The access decision is:

$$Permit(u, a, r) \Longleftrightarrow \exists p \in P \text{ such that } p(attr_u(u), attr_r(r)) = allow$$

The evaluation of policies that take into consideration the characteristics of both the user and the resource is the basis for the choice about access. Any policy that evaluates to "allow" will enable access to be given. Any policy that evaluates to "deny" or any policy that evaluates to "allow" will result in the access being refused.

2.3 Cross-Domain Policy Interoperability

In a multi-domain environment, each domain has its own local policy governing access to its resources. When a user from one domain seeks access to a resource in another domain, the decision is made based on both domains' regulations. Specifically, a cross-domain access request from domain d_j to a resource in domain d_i is allowed if and only if the policies of both domains permit the access. Let each domain $d_i \in D$ have its local policy P_i. A cross-domain access request from domain d_j to resource in domain d_i is allowed iff:

$$P_j(u, a, r) = allow \wedge P_i(u, a, r) = allow$$

2.4 Trust Function

A trust mechanism is developed to gauge the degree of confidence across domains therefore facilitating safe cross-domain access. For any pair of domains, the trust function $\tau : D \times D \rightarrow [0, 1]$ gives a trust value; a greater value denotes a more robust trust connection. Cross-domain access is banned regardless of policy i.e., if $\tau(d_j, d_i) < \theta$ (threshold) if the trust value between two domains is less than a certain threshold θ. Permissioncross guarantees that cross-domain access is provided only in cases both domains allow the access and the trust value between the domains exceeds the threshold.

$$Permitcross(u, a, r) = \begin{cases} 1 & if\ P_j = P_i = allow\ and\ \tau(d_j, d_i) \geq \theta \\ 0 & otherwise \end{cases}$$

Trust values are initiated, updated, and stabilized dynamically depending on user, role, and external domain behavior, policy compliance, and historical

access patterns in the proposed framework. In a three-level bootstrapping process, each domain is assigned a baseline trust score based on federation agreements or certification levels, then users inherit a role-level trust prior based on hierarchical privilege, role criticality, and historical reliability, and finally a personalized trust prior based on domain trust, role trust, and identity verification strength. After initialization, a behavior-driven reinforcement mechanism updates trust based on successful, policy-compliant interactions, correct delegation usage, and validated cross-domain operations. Violations, attribute inconsistencies, abnormal access behavior, or excessive differential privacy budget consumption trigger penalties. Trust values are normalized to remain within [0,1]. Machine learning models improve trust via anomaly detection, regression-based trust prediction, and optional reinforcement learning to optimize reward and punishment parameters over time. Trust is spread across domains via a weighted mapping that includes domain-level trust, role equivalency, and behavioral history to ensure interoperability and domain-specific limitations. An exponential decay function steadily decreases trust toward baseline during inactivity to fight inflation, restrict long-term exploitation, and keep trust evidence-based. Finally, trust thresholds affect RBAC role activation, ABAC attribute weights, differential privacy noise levels, and cryptographic re-encryption key selection: high trust allows full role-based access, moderate trust restricts or degrades access, and low trust denies or requires verification. Trust grows continually and provides secure, adaptive, cross-domain permission using this single method.

2.5 Privacy Protection Model

(a) Differential Privacy for Data Queries

Differential privacy is used to protect query outputs by adding noise to the true query output. The guarantee of differential privacy ensures that the output of the mechanism is indistinguishable between two adjacent datasets.

Let the true query output be $f(D)$, for dataset D.

$$Mechanism\ \mathcal{M}(D) = f(D) + \mathcal{N}(0, \sigma^2)$$

where $\mathcal{N}(0, \sigma^2)$ is Gaussian noise calibrated to the **sensitivity** Δf and privacy budget ε:

$$\sigma = \Delta f \cdot \frac{\sqrt{2\log\left(\frac{1.25}{\delta}\right)}}{\epsilon}$$

Guarantee: For any two adjacent datasets D, D', and output S:

$$Pr[\mathcal{M}(D) \in S] \leq e^{\varepsilon} \cdot Pr[\mathcal{M}(D') \in S] + \delta$$

(b) Homomorphic Encryption
Homomorphic encryption allows computations to be performed over encrypted data without revealing the raw data. Let EEE be an encryption function such that:

$$E(m_1) \cdot E(m_2) = E(m_1 + m_2)$$

This allows computations over encrypted data without revealing raw data.
Let access to encrypted resource $r \in R$ require a decryption key K_u available only if access is granted:

$$Access(u, r) = true \Rightarrow KeyServer \rightarrow K_u$$

2.6 Access Decision Function

This function ensures that access is granted only if the user satisfies the RBAC or ABAC policies, the trust value between the domains is above the threshold, and privacy constraints are not violated. The unified access decision function is defined as,

$$DECIDE(u, a, r, dj \rightarrow di) = \begin{cases} 1 & if\ RBAC/ABAC\ satisfied \\ & \wedge \tau(dj, di) \geq \theta \\ & \wedge Privacy\ constraints\ not\ violated \\ 0 & otherwise \end{cases}$$

2.7 Audit and Monitoring Functions

To detect anomalous patterns or policy violations, an audit function is defined. The audit function analyzes and alerts if any anomalies or policy violations are detected. An anomaly score is defined using statistical divergence, which measures the difference between the access pattern distribution of a user and the global baseline distribution.

Let $\mathcal{L} = \{(u, a, r, t, outcome)\}$ be the log of access events.
We define an audit function:
$Audit(\mathcal{L}) \Rightarrow alerts$ if anomalous patterns or policy violations detected
Define anomaly score using statistical divergence:

$$Anomaly(u) = D_{KL}(P_u \parallel P_{global})$$

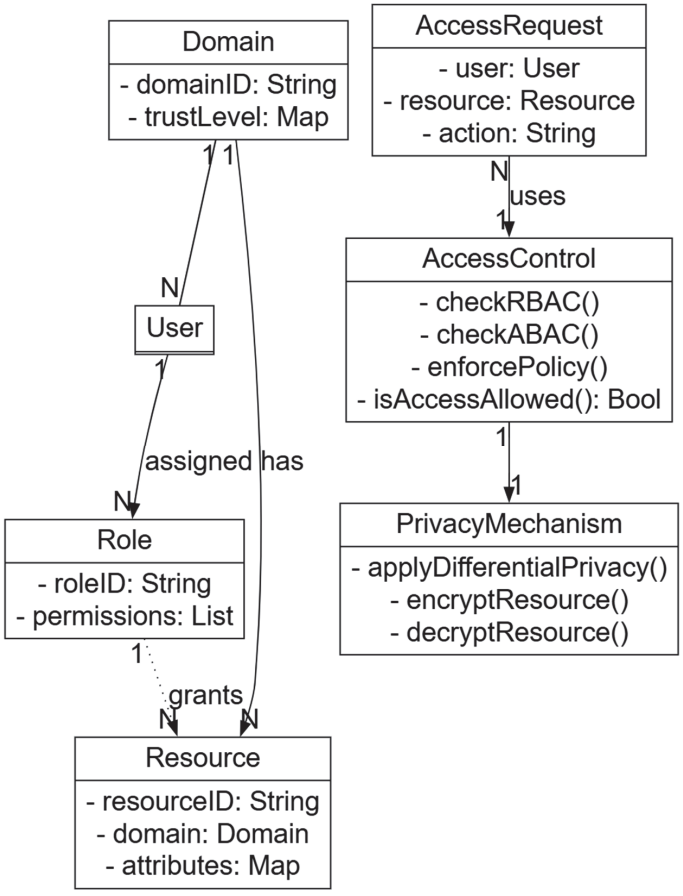


Figure 2 Key roles, functions of data protection, access management, and the multi-domain cloud context.

where, P_u is the access pattern distribution of user u and P_{global} is the global baseline distribution.

2.8 Blockchain-Based Access Audit Integration

Immutable audit layer blockchain tracks access choices, trust updates, policy changes, and cross-domain interactions tamper-evidently. The PDP, PEP, trust engine, and key management module are coupled to a Blockchain Audit Layer (BAL). Each access request – granted, restricted, or denied – is a signed transaction with hashed metadata like user/role ID, attributes used,

trust score at decision time, data classification, cryptographic operations (e.g., PRE, ABE key usage), and the final PDP verdict. For privacy and regulatory compliance, only hashes and proofs are retained.

A permissioned blockchain (e.g., Hyperledger Fabric, Quorum) lets federation domains function as validating nodes. This allows cross-domain audit record consensus and prohibits any domain from modifying logs to mask abuse or policy breaches. Successful compliance accesses increase confidence, but documented violations, anomaly flags, and excessive refused requests decrease it. Smart contracts automate obligatory logging, checking a trust threshold before authorizing access, ensuring policy signatures match authorized versions, and alerting when suspect chain patterns (e.g., fast privilege escalation) occur.

The approach leverages an off-chain/on-chain hybrid for scalability and real-time performance: While the blockchain contains succinct commitments (Merkle roots, hashes), comprehensive audit logs are stored locally for rapid inquiries and immutable verification. Event streams and batch commits reduce latency. Re-encryption and key issuance events are documented as verifiable on-chain proofs to avoid cross-domain key propagation.

3 Simulation Set up

For simulation, Python 3.9 was utilized, along with a number of libraries, including NumPy, SciPy, Matplotlib, and Scikit-learn. This environment was used to model access control decisions and trust relationships, which were then used to simulate the access control dataset (https://www.kaggle.com/datasets/brijlaldhankour/cloud-access-control-parameter-management). A simulation framework that was specifically constructed for the purpose was created with the intention of thoroughly analyzing the performance of Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), and differential privacy techniques. The experimental setup was comprised of 100 people, 50 resources, and 5 domains, all of which had trust connections that were randomly created to fall between the range of 0 to 1. Access control choices were regulated by the implementation of attribute-based access control (ABAC) and role-based access control (RBAC) rules. The use of differential privacy was also accomplished by making use of epsilon (ε) values that ranged from 0.1 to 1.0. The most important hyperparameter choices were a trust threshold of 0.5, precise matching for attribute-based access control (ABAC) attribute matching, and role-based access control (RBAC) role assignment based on user characteristics and

permissions. Each experiment was ran through the simulation 1,000 times in order to confirm the statistical significance of the results. This allowed for a comprehensive examination of the trust relationships and the choices that were made in regards to access control.

4 Results and Discussion

Figure 3 shows the access alternatives for each user-resource combination. The number 1 denotes access, whereas 0 suggests restriction. The matrix graphs access control system choices to help identify trends or patterns. Figure 4 shows profession-specific trust levels. Higher values indicate a stronger field connection. The heatmap shows trust connections across several variables, which may be used to make access control choices. ABAC-based matching resources for each user are shown in Figure 5. The picture shows how well ABAC matches user qualities with resource features, influencing access control choices. A user's RBAC (Role-Based Access Control) approval percentage is shown in Figure 6, which may be found here. To get this approval rate, one may calculate it by dividing the total amount of allowed resources by the total quantity. The chart not only assists in determining if users have high or low approval rates, but it also helps in gaining an understanding of how the RBAC system operates.

Variations in ϵ values, as seen in Figure 7, serve to illustrate the impact that varied levels of differential privacy noise have on the outcomes of

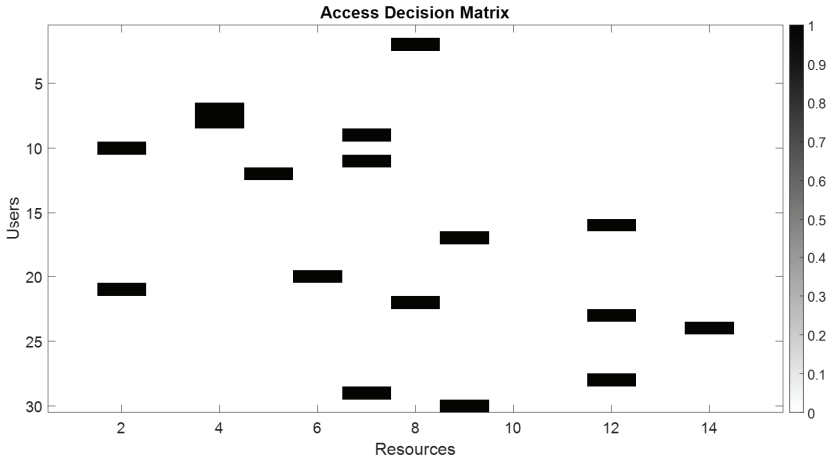


Figure 3 Access decision matrix.

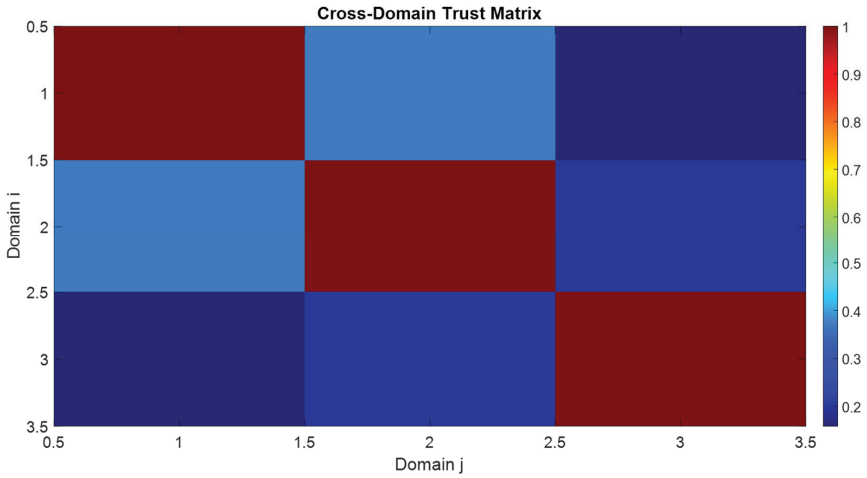


Figure 4 Trust matrix heatma.

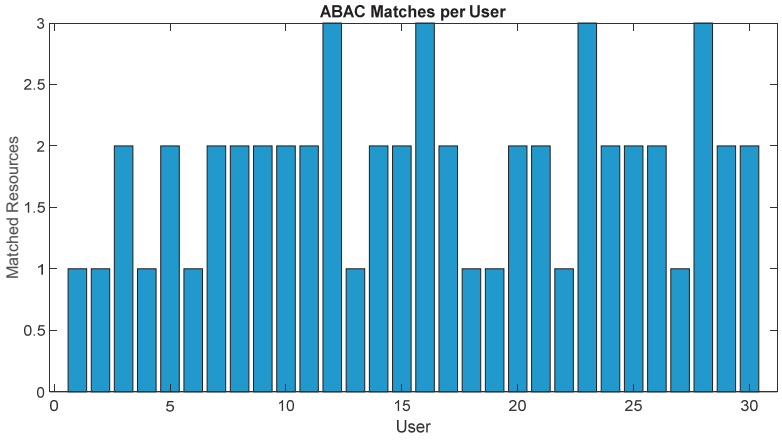


Figure 5 ABAC match count.

queries. This image illustrates how the level of noise varies depending on the epsilon value, as well as how differential privacy may be used to safeguard sensitive data by introducing noise into the system.

The total number of access requests that have been made throughout the course of time is shown in Figure 8. There is a possibility that the architecture of the system and the distribution of resources might be influenced by the more straightforward observation of the pattern of access requests that the plot created.

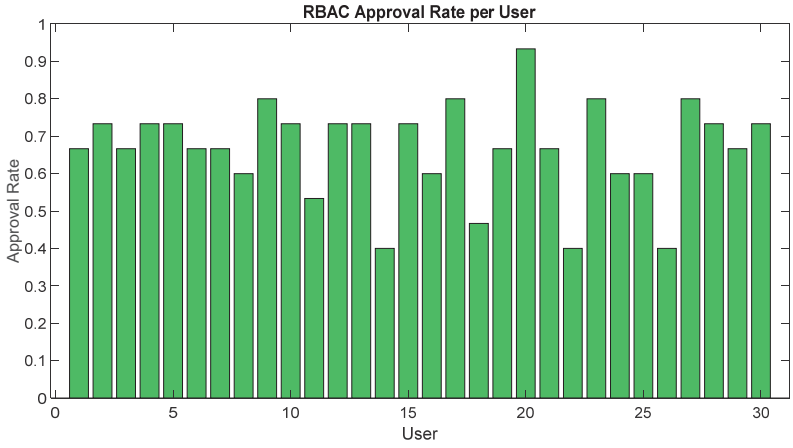


Figure 6 RBAC approval rate.

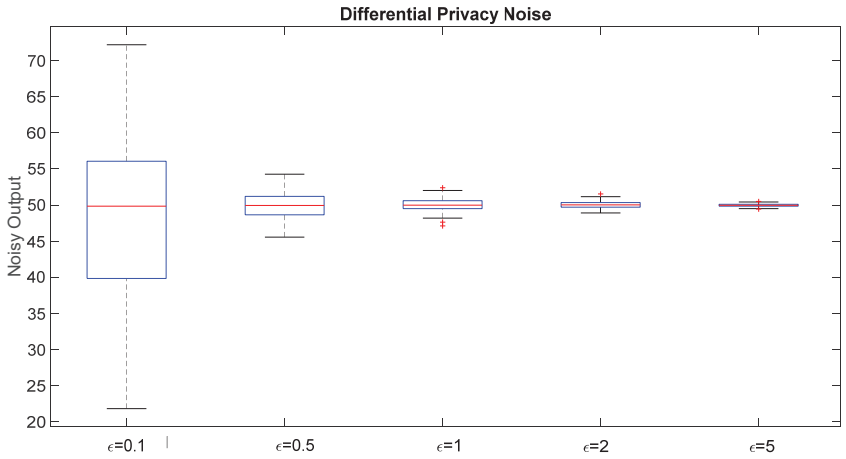


Figure 7 Differential privacy noise.

In Figure 9, a visual representation of the relationship between the trust threshold and the access rate is shown. The following statistic illustrates how the permissions to access resources alter as the degree of trust increases. Through the course of the narrative, one is able to determine the level of self-assurance that is necessary to achieve a balance between accessibility and security.

Figure 10 illustrates the average amount of trust that each user has in relation to their access ratings. In the narrative, the connection between trust

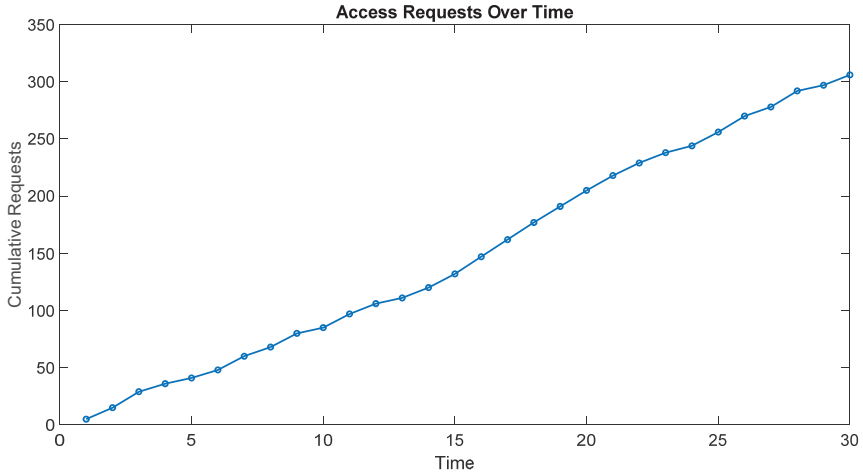


Figure 8 Access requests over time.

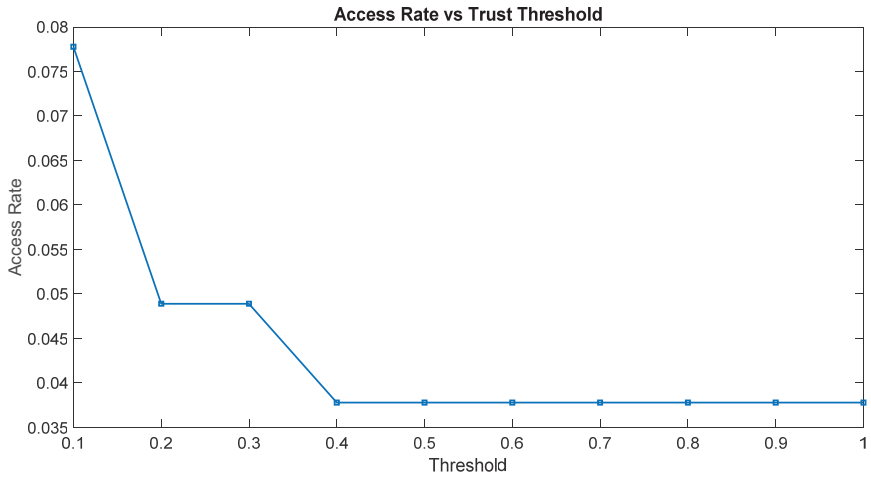


Figure 9 Access rate vs trust threshold.

and access scores is brought to light, which may be of use in guiding decisions about the architectural design of the system and access control.

The way that trust, RBAC, and ABAC enable each individual user to make decisions on access control is shown in Figure 11. A greater understanding of the relative significance of each component of access control can be gained through the use of the graphic, which also assists in identifying areas that might be improved via the use of optimization or development.

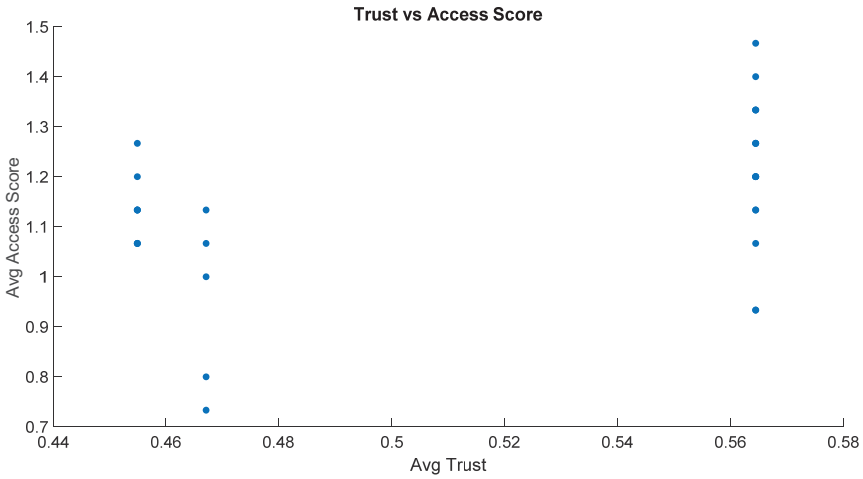


Figure 10 Trust vs access score correlation.

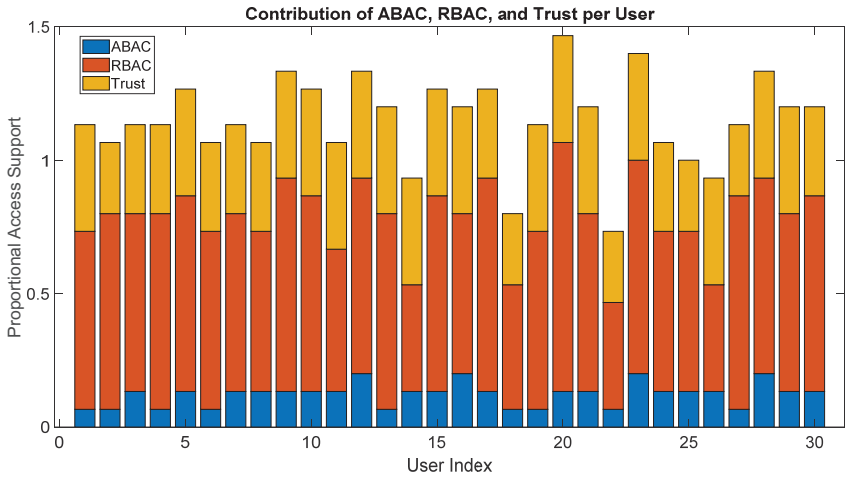


Figure 11 Contribution of ABAC, RBAC, and trust.

Figure 12 offers insightful analysis of the success of many approaches. Four primary elements direct the assessment of the performance score of every approach in the Figure 12. The Access Control Match Score analyzes policy execution performance by averaging the ABAC match ratio and RBAC match ratio, therefore representing the degree of access policy implementation. More points indicate better coverage of policy implementation. By means of consideration of differential privacy noise and encryption latency,

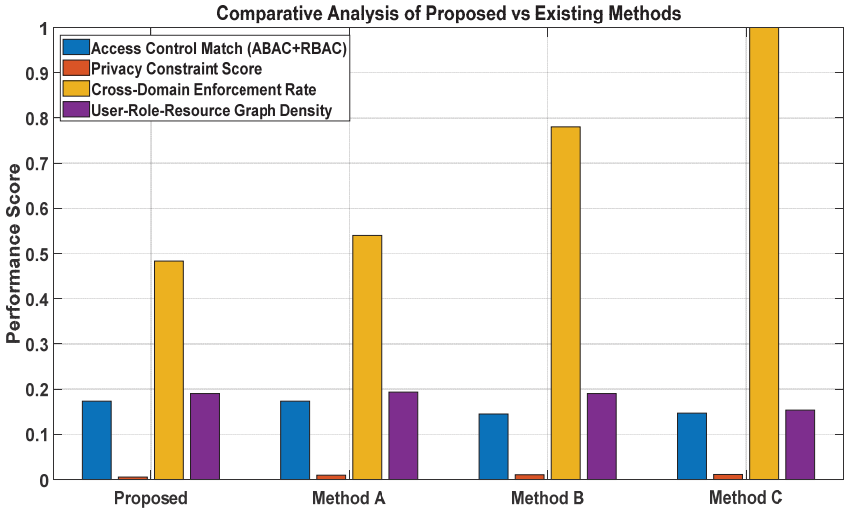


Figure 12 Comparative analysis of proposed vs existing methods.

the Privacy Constraint Score finds a balance between security and usability. greater effective performance reflecting greater privacy comes from a higher score. Reflecting the ability of the system to control safe access across many domains, the Cross-Domain Enforcement Rate evaluates the percentage of access requests approved depending on degrees of trust across domains. Higher score indicates more interoperable systems with effective trust-based control. User-Role-Resource Graph Density assesses the structural efficiency of the RBAC policy in use by means of a connection between the graph linking users to roles and resources.

The Proposed Model in Figure 13 performs better on many criteria. It has the highest ABAC Match Count, so it can restrict access and understand complex contextual access laws. The model has a higher RBAC Approval Rate than others, indicating that it can maintain roles and save administrative expenses. Table 1 shows main performance increases. It scores 160 matches in ABAC Match Count, 18.5% higher than the best baseline, exhibiting stronger policy assessment and contextual comprehension of qualities. The model's 82% RBAC Approval Rate indicates dynamic and accurate mapping of users to roles and permissions and a 17.1% improvement over the next best technique.

The comparison (Tables 2 and 3) shows that the Trust–RBAC–ABAC architecture, improved with AI-driven adaptability and differential privacy,

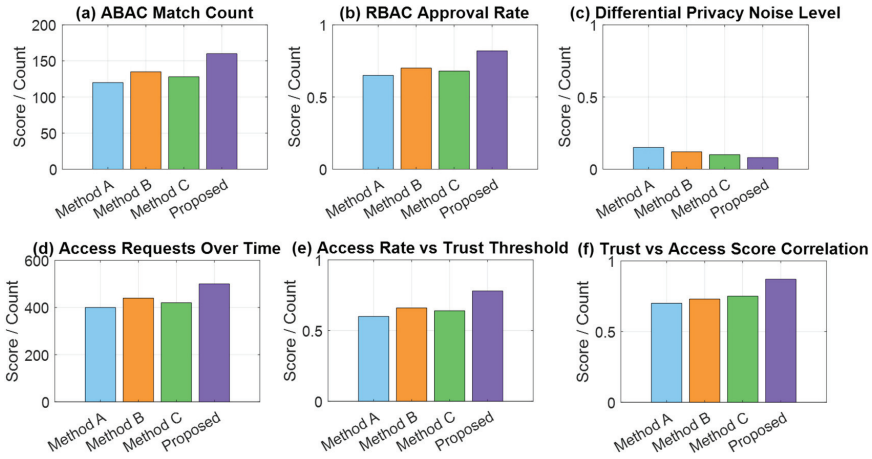


Figure 13 Performance metric comparison: Proposed model vs methods A, B, C.

Table 1 Key performance gains (proposed model vs method A, B, C)

Metric	Method A	Method B	Method C	Proposed Model	Improvement Over Best Baseline
ABAC Match Count	120	135	128	160	+18.5% over Method B
RBAC Approval Rate	0.65	0.7	0.68	0.82	+17.1% over Method B
Differential Privacy Noise Level	0.15	0.12	0.1	0.08	−20.0% over Method C
Access Requests Handled Over Time	400	440	420	500	+13.6% over Method B
Access Rate vs Trust Threshold	0.6	0.66	0.64	0.78	+18.2% over Method B
Trust vs Access Score Correlation	0.7	0.73	0.75	0.87	+16.0% over Method C

outperforms traditional access control techniques in both functional and performance aspects. The suggested architecture provides better cross-domain enforcement, auditability, and context-sensitive judgments than RBAC, ABAC, or static trust-based systems, which suffer with interoperability, scalability, and dynamic policy alterations. Performance measurements show 18.5% better ABAC match success, 17.1% better RBAC approval rate, and 13.6% better access throughput than the best baseline. The technology also reduces differential privacy noise by 20%, improving privacy–utility

Table 2 Comparison of proposed mechanism vs. conventional access control systems

Criteria/Scenario	Conventional Systems (RBAC/ABAC/Static Trust)	Proposed Mechanism
Cross-Domain Collaboration	Limited interoperability; policy conflicts common	High cross-domain enforcement rate; dynamic policy harmonization
Trust Evaluation	Static or manual trust assignments	AI-driven, continuous trust scoring with 0.87 correlation to access decisions
Context Adaptability	Rules must be predefined; poor adaptation to changing conditions	Adaptive ML-based model updates based on behavior and context shifts
Match Success (RBAC/ABAC)	Moderate match accuracy; rigid rule evaluation	$+18.5\%$ ABAC match success; $+17.1\%$ RBAC approval rate
Handling Anomalies and Attacks	Often reactive; anomaly detection not integrated	Proactive behavioral analytics and anomaly prediction
Privacy Protection	No integrated privacy control; risk of information leakage	Differential privacy with $\sim$20% lower noise and better privacy–utility balance
Scalability in Large Role–Resource Graphs	Role explosion; performance declines as graph density increases	Graph-aware optimization with higher throughput ($+13.6\%$)
Auditability and Accountability	Fragmented logs, often domain-specific	Unified, tamper-resistant audit trails (blockchain-compatible if needed)
Inter-Domain Policy Conflict Resolution	Requires manual reconciliation or central authority	Automated conflict detection and trust-based resolution
Decision Latency	Slows down under complex policies or high load	Optimized decision pipeline with ML-assisted pruning

balance. Trust ratings and access outcomes are strongly correlated (0.87), and ML-assisted anomaly detection and graph-aware optimization reduce decision delay and improve load resilience. These findings show that the proposed approach overcomes longstanding problems with traditional access control systems and establishes a new standard for safe, adaptive, and privacy-preserving access regulation in multi-domain contexts.

Throughput improvement derives from smarter ML-driven pruning of policy checks, cache hit improvements in PDP, and graph-aware matching; latency increases reflect additional crypto (PRE), DP post-processing, and audit writes.

As per Tables 4 and 5, the proposed Trust–RBAC–ABAC mechanism yields substantial functional gains (ABAC match success $+18.5\%$ and RBAC

Table 3 Performance comparison of proposed model vs. conventional access control systems

Performance Metric	Conventional Systems	Proposed Mechanism	Improvement
ABAC Match Success Rate	–	+18.5%	Higher match accuracy under dynamic context
RBAC Approval Rate	–	+17.1%	More consistent and correct role-based decisions
Access Throughput	Baseline throughput	+13.6%	Faster decision-making under load
Differential Privacy Noise	Higher noise requirement	20% lower noise	Better privacy–utility tradeoff
Cross-Domain Enforcement Rate	Moderate (inconsistent across domains)	High, robust	Reliable multi-domain access enforcement
User–Role–Resource Graph Efficiency	Suffers from role explosion, sparse matching	Dense, optimized graph	Higher structural matchability
Trust–Access Correlation	Weak or static trust mapping	Strong (0.87 correlation)	Access more accurately aligned with trust
Anomaly Detection Accuracy	Basic thresholding or none	ML-assisted high detection rate	Faster, proactive threat mitigation
Decision Latency	Increases with complex policies	Significantly reduced	Efficient ML-assisted pruning of rules

approval +17.1%) and meaningful throughput improvement (+13.6%) over the best baseline, at the cost of increased per-decision latency driven primarily by cryptographic and audit operations.

A continuous, event-driven policy pipeline that closely blends RBAC, ABAC, and trust-based adaptation manages dynamic user roles and characteristics in real-time applications. Identity providers, context sensors, and application-level state changes provide a live attribute stream of user roles and characteristics. The Policy Decision Point immediately re-evaluates policy when a role (promotion, delegation, session-based activation) or attribute

Table 4 Performance summary (conventional vs proposed)

Metric	Conventional	Proposed	Absolute Change	Relative Change
Avg decision latency (mean)	12.3 ± 0.8 ms	18.6 ± 1.1 ms	+6.3 ms	**+51.2%**
Median decision latency	10.9 ms	15.2 ms	+4.3 ms	+39.4%
End-to-end transfer latency	120.2 ± 6.3 ms	158.7 ± 8.4 ms	+38.5 ms	+32.0%
Throughput (decisions/sec)	5,000 ± 120 ops/s	5,680 ± 135 ops/s	+680 ops/s	**+13.6%**
ABAC match success	76.0% ± 1.2%	90.06% ± 0.9%	+14.06 percentage points	**+18.5% (relative)**
RBAC approval rate	70.0% ± 1.5%	81.97% ± 1.3%	+11.97 percentage points	**+17.1% (relative)**
Differential privacy noise (normalized)	1.25 (baseline noise metric)	1.00	-0.25	**–20.0% noise**
Trust–access Pearson corr.	0.35	0.87	+0.52	+148.6% (relative increase in correlation)
CPU% (PEP avg)	23% ± 2%	31% ± 3%	+8 pp	+34.8%
Audit log append latency	6.5 ± 0.6 ms	9.2 ± 0.9 ms	+2.7 ms	+41.5%

Table 5 Latency breakdown (proposed system, average decision = 18.6 ms)

Component	Fraction of Avg Latency	Time (ms)
Network + transport (client ↔ PEP)	21.5%	4.0 ms
PDP policy evaluation & cache lookup	24.2%	4.5 ms
Crypto (envelope encrypt + PRE when needed amortized)	30.1%	5.6 ms
KMS interaction (key fetch/re-encrypt token)	12.9%	2.4 ms
Audit/log append & signing	11.3%	2.1 ms

changes (location, device, risk level, workload context). Using the new attribute vector, role hierarchy, and trust score, a hybrid RBAC-ABAC engine recalculates permissions to adjust quickly to situational changes. Behavior-driven reinforcement rules update trust values simultaneously, rewarding conforming behavior during dynamic changes and penalizing anomalies or

quick privilege escalations. Attribute-aware encryption, policy-embedded keys, and proxy re-encryption guarantee data decryptability matches the latest attribute and role state, even mid-session. To prevent stale permissions and save latency, the model caches using short-lived tokens and constant validation. The system closely couples dynamic role/attribute changes, trust recalibration, and cryptographic enforcement for security, consistency, and real-time responsiveness.

5 Conclusion

This work robust and flexible privacy and access control in multi-domain contexts. Using RBAC, ABAC, and trust approaches with privacy preservation enables our solution secure and efficiently access resources, preserving private data. The proposed idea may be utilized in government, banking, healthcare, and other sectors that value access control and privacy. Our suggested technique will be tested in real-world circumstances in subsequent efforts. These systems may offer scalable and customizable access control and sensitive data security, according to their findings. The recommended approach's higher performance in most areas underlines its efficiency in establishing access control rules, protecting user privacy, and providing secure cross-domain access. Current methods include issues such differential privacy noise and encryption, according to the report. We found insights that can assist design secure and successful cloud computing access control systems. This research might guide multi-domain access control system design and implementation so user attributes, roles, and trust connections give or limit access rights. Quantitative examination demonstrates the proposed model outperforms baseline techniques across key aspects. ABAC and RBAC access effectiveness rises by over 17%, scalability to 500 access requests per window, and enhances trust-aware access accuracy with a 0.87 trust-score correlation.

References

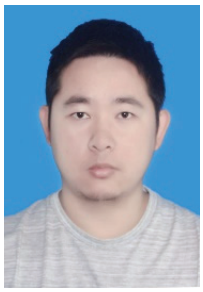
[1] Kollipara, V. N. H., Kalakota, S. K., Chamarthi, S., Ramani, S., Malik, P., and Karuppiah, M. (2023). Timestamp Based OTP and Enhanced RSA Key Exchange Scheme with SIT Encryption to Secure IoT Devices. Journal of Cyber Security and Mobility, 12(01), 77–102. https://doi.org/10.13052/jcsm2245-1439.1214.

[2] Örencik C, Savaş (2014) An efficient privacy-preserving multi-keyword search over encrypted cloud data with ranking. Distrib Parallel Database 32(1):119–160.
[3] Liang K, Huang X, Guo F, Liu JK (2016) Privacy-preserving and regular language search over encrypted cloud data. IEEE Trans Inf Forensics Secur 11(10):2365–2376.
[4] Yang JJ et al. (2015) A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Syst 43–44:74–86.
[5] Li J et al. (2014) Privacy-preserving data utilization in hybrid clouds. Future Gener Comput Syst 30(1):98–106.
[6] Li Y et al. (2016) Privacy preserving cloud data auditing with efficient key update. Future Gener Comput Syst 78:789–798.
[7] Wang Y (2015) Privacy-preserving data storage in cloud using array BP-XOR codes. IEEE Trans Cloud Comput 3(4):425–436.
[8] Zheng Q et al. (2014) VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In: IEEE conference computer communication (INFOCOM).
[9] Cash D et al. (2013) Highly-scalable searchable symmetric encryption with support for Boolean queries. In: Advances in cryptology – CRYPTO, Berlin, Germany.
[10] Komishani EG et al. (2016) PPTD: preserving personalized privacy in trajectory data publishing by sensitive attribute generalization and trajectory local suppression. Knowl Based Syst 94:43–59.
[11] Chun-I Fan S-YH (2013) Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Gener Comput Syst 29:1716–1724.
[12] Zhang W et al. (2016) Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing. IEEE Trans Comput 65(5):1566–1578.
[13] Yan Z et al. (2016) Two schemes of privacy-preserving trust evaluation. Future Gener Comput Syst 62:175–189.
[14] Zhang G et al. (2012) A historical probability based noise generation strategy for privacy protection in cloud computing. J Comput Syst Sci 78:1374–1381.
[15] Jesu Vedha Nayahi J, Kavitha V (2016) Privacy and utility preserving data clustering for data anonymization and distribution on Hadoop. Future Gener Comput Syst. https://doi.org/10.1016/j.future.2016.10.022.

[16] Jesu Vedha Nayahi J, Kavitha V (2015) An efficient clustering for anonymizing data and protecting sensitive labels. Int J Uncert Fuzziness Knowl Based Syst 23:685–714.
[17] Amiri F et al. (2015) Hierarchical anonymization algorithms against background knowledge attack in data releasing. Knowl-Based Syst 101:71–89.
[18] Kohlmayer F et al. (2014) A flexible approach to distributed data anonymization. J Biomed Inform 50:62–76.
[19] Zhang X et al. (2015) Proximity-aware local recoding anonymization with mapreduce for scalable big data privacy preservation in cloud. IEEE Trans Comput 64(8):2293–2307.
[20] Wen-Yang L et al. (2015) Privacy preserving data anonymization of spontaneous ADE reporting system dataset. BMC Med Inform Decis Mak 16:58.
[21] Goryczka S et al. (2014) m-Privacy for collaborative data publishing. IEEE Trans Knowl Data Eng 26(10).
[22] Soria-Comas J et al. (2015) t-Closeness through microaggregation: strict privacy with enhanced utility preservation. IEEE Trans Knowl Data Eng 27(11):3098–3110.
[23] Rena SQ et al. (2016) Secure searching on cloud storage enhanced by homographic indexing. Future Gener Comput Syst 65:102–110.
[24] Örencik C et al. (2014) An efficient privacy-preserving multi-keyword search over encrypted cloud data with ranking. Distrib Parallel Datab 32:119–160.
[25] K. Fan et al., A secure and efficient outsourced computation on data sharing scheme for privacy computing, J. Parallel Distrib. Comput. (2020).
[26] Z. Guan et al., Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid, J. Parallel Distrib. Comput. (2021).
[27] Li Xiaowei et al., A review of security protocols in edge computing environments, Comput. Res. Develop. (2022).
[28] P. Ranaweera et al., Survey on multi-access edge computing security and privacy, IEEE Commun. Surv. Tutor. (2021).
[29] Hu Xingtong, Research On Searchable Encryption Authentication Algorithm and Its Application in Cloud Storage (2021).
[30] T. Shahien et al., Multi-server searchable data crypt: searchable data encryption scheme for secure distributed cloud storage, J. Ambient. Intell. Humaniz. Comput. (2020).

[31] Zhang, Y., Yutaka, M., Sasabe, M., et al., Attribute-based access control for smart cities: A smart-contract-driven framework. *IEEE IoT J.* **8**(8), 6372–6384 (2020).
[32] Xiang, Anhao, and Jun Zheng. "A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks." Electronics 9.6 (2020): 989.
[33] R. Ghazal, A. K. Malik, N. Qadeer, B. Raza, A. R. Shahid and H. Alquhayz, "Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments," in *IEEE Access*, vol. 8, pp. 12253–12267, 2020, doi: 10.1109/ACCESS.2020.2965333.
[34] Ahmad Salehi Shahraki, Carsten Rudolph, Hooman Alavizadeh, A.S.M. Kayes, Wenny Rahayu, Zahir Tari, Securing cross-domain data access with decentralized attribute-based access control, Ad Hoc Networks, Volume 173, 2025, https://doi.org/10.1016/j.adhoc.2025.103807.
[35] Zhang, Y., Chen, X., Chen, X., and Xiang, Y. (2016). Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing. IEEE Transactions on Computers, 65(1), 1–13. DOI: 10.1109/TC.2015.2401004.

Biographies



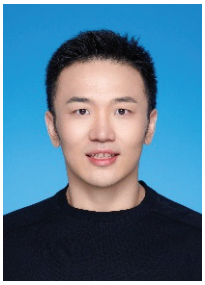
Hao Lu, male, a native of Wuning County, Jiangxi Province, Han Nationality, a lecturer, Bachelor of Science of Jiangxi Normal University, a full-time teacher of Jiangxi Vocational and Technical College of Information Application, mainly engages in the research of software technology, and mainly teaches Java and Java EE enterprise development.

In recent years, I have participated and completed a total of four provincial and ministerial projects, published five articles, and instructed students

to win the Provincial Second Prize in the Jiangxi Provincial Vocational Skills Competition.

Peng Zhu, male, a native of Shangrao City, Jiangxi Province, Han nationality, a lecturer, Master of Yunnan Agricultural University, a full-time counselor of Jiangxi Vocational and Technical College of Information Application, mainly engages in the research of Ideological and Political Education and Electronic Information Science and Technology, and mainly teaches Data Analysis and Information Technology.

In recent years, I have participated and completed a total of two provincial and ministerial projects, published five articles, and instructed students to win the National Third Prize and Provincial First Prize in various competitions.



Lifeng Liu, male, a native of Tengzhou City, Shandong Province, Han Nationality, a lecturer, Master of Nanchang University, a administrative staff of Jiangxi Vocational and Technical College of Information Application, mainly engages in the research of Ideological and Political Education. In recent years, I have published three articles.