International Journal of Computer Techniques – IJCT Volume 12 Issue 5,October 2025

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

An Improved Mechanism for Access Control using Context Awareness

Taylor, Onate Egerton
Department of Computer Science *(Rivers State University)*
Port-Harcourt, Rivers State, Nigeria
ORCID: 0000-0003-4477-9987

*Davies, Isobo Nelson
Department of Computer Science *(Rivers State University)*
Port-Harcourt, Rivers State, Nigeria
ORCID: 0009-0006-6421-339X

Abstract
Access control remains a critical security mechanism in modern computing environments, yet traditional models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) are increasingly inadequate for dynamic distributed systems and their environments. These conventional approaches rely on static roles and permissions that fail to adapt to contextual factors such as user location, device trust levels, network conditions, and temporal constraints. This paper presents an Improved Context-Aware Access Control Mechanism (ICAACM) that integrates real-time contextual information with fuzzy logic-based decision making to address the limitations of existing access control models. The proposed mechanism employed a four-layer architecture comprising User and Device, Context Acquisition, Decision-Making, and Enforcement layers. The system utilized Mamdani fuzzy inference to compute a Contextual Risk Score (CRS) based on six key parameters: location, time, device trust, network security, user activity, and risk indicators. Experimental evaluation using a simulated dataset of 10,000 access requests demonstrates that the ICAACM achieved superior performance with 95.70% accuracy, 5.20% False Acceptance Rate (FAR), and 6.10% False Rejection Rate (FRR), representing significant improvements of 7.5%, 2.7%, and 4.25% over RBAC, RAdAC, and ABAC respectively. The mechanism maintained computational efficiency with an average decision latency of 7.3ms while consuming reasonable system resources of 13.7% CPU usage, and 230MB memory. Further, the scalability analysis demonstrates linear performance degradation with system load, maintaining sub-10ms response times for up to 1000 concurrent requests. The results indicated that the ICAACM provides a robust, adaptive, and efficient solution for access control in modern distributed computing environments where traditional static models prove insufficient.

Keywords— Access Control, Context Awareness, Fuzzy Logic, Risk Assessment, Cybersecurity, Distributed Systems

I. INTRODUCTION

Access Control remains one of the most fundamental and widely deployed security mechanisms for ensuring security and privacy in computing environments [1]. As digital transformation accelerates, enterprises, governments, and individuals increasingly rely on distributed computing platforms for sensitive transactions and data processing [2]. This dependency has exposed critical limitations in traditional access control models, creating an urgent need for adaptive and context-aware security mechanisms [3].

Traditional access control models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) operate on static principles that do not adequately address the dynamic nature of modern computing environments [4]. These systems fail to consider contextual factors such as temporal variations, geographical constraints, device trust level, behavioral anomalies, and environmental risk factors [5, 6].

Recent cybersecurity reports indicate that inadequate access control mechanisms contribute to 43% of all security breaches, with insider threats representing 34% of security incidents. The average cost of a data breach has increased to $4.45 million in 2024, highlighting the critical need for more sophisticated contextual access control mechanisms. The traditional models are not well-equipped to capture and evaluate contextual factors. This often leads to unauthorized access, insider misuse, or legitimate requests being denied [7]. Attribute-Based Access Control (ABAC) and Risk-Adaptive Access Control (RAdAC) have attempted to address some of these limitations by incorporating user and environmental attributes. However, they still face challenges in terms of handling uncertainty, dynamic adaptation, computational overhead, and fine-grained decision-making [8].

Context-awareness has emerged as a promising paradigm for addressing these limitations of conventional systems. A context-aware access control system extends beyond static roles and attributes by incorporating real-time contextual information into decision-making [9]. For example, a healthcare professional accessing patient records during working hours from a hospital's secure network may be granted full access, while the same request outside of working hours or from an unrecognized device may trigger partial access or multi-factor authentication. This adaptive approach ensures that access control decisions are not only based on identity or role, but also on the situational context in which the request is made [10].

Nonetheless, despite progress in context-aware access control models, existing solutions often fall short in delivering a mechanism that is scalable, lightweight, risk-aware, and capable of managing uncertainty in real-world environments [11]. Many approaches also fail to achieve an optimal balance between security, usability, and system performance. This creates a pressing need for an improved access control

mechanism that dynamically incorporates contextual information while maintaining efficiency and reliability.

Presented in this paper is an Improved Context-Aware Access Control Mechanism (ICAACM) designed to integrate contextual information into a unified security decision engine, effectively addressing identified limitations through several key objectives. These objectives include the design of a comprehensive context-aware access control architecture that incorporates multiple contextual parameters, the development of a mathematical model utilizing fuzzy logic to manage uncertainty in contextual data, the implementation of an adaptive decision-making mechanism that balances security with usability, the evaluation of the proposed mechanism against existing models using detailed performance metrics, and the demonstration of its practical applicability and scalability.

The primary contributions of this work are highlighted by a novel four-layered context-aware access control architecture that seamlessly merges traditional rule-based controls with dynamic context evaluation, the integration of a Mamdani fuzzy inference system to effectively handle uncertainty in contextual parameters, and an adaptive, dynamic risk assessment mechanism that adjusts access decisions based on real-time contextual factors.

II. RELATED WORK

The evolution of access control mechanisms has been driven by the increasing complexity of computing environments and the need for more sophisticated security models. This section provides a comprehensive review of existing approaches, organized thematically to highlight the progression from static to dynamic access control mechanisms.

A. Traditional Access Control Models

Early access control models focused on identity-based authentication and static permission assignment. Discretionary Access Control (DAC) allows resource owners to determine access rights, providing flexibility but often leading to inconsistent policy enforcement [12]. Mandatory Access Control (MAC) enforces strict hierarchical security classifications, offering high security but limited flexibility for dynamic environments [13].

Role-Based Access Control (RBAC) emerged as a significant advancement, simplifying administration by assigning permissions based on organizational roles rather than individual identities [14]. Despite widespread adoption and NIST standardization, RBAC's static nature limits its effectiveness in modern distributed environments where context plays a crucial role in access decisions [15].

B. Attribute-Based Access Control Evolution

Recognizing RBAC's limitations, Attribute-Based Access Control (ABAC) introduced fine-grained access control using attributes of users, resources, environment, and actions [16]. ABAC provides greater flexibility and granularity compared to RBAC, enabling more sophisticated policy definitions. However, ABAC implementations face challenges including policy explosion, high computational overhead, and complex conflict resolution mechanisms [17].

Recent research by [17] introduced ABAC Lab, an interactive platform for policy analysis, highlighting ongoing efforts to address ABAC's complexity challenges. Their work demonstrates the need for better tools and frameworks to manage attribute-based policies effectively.

C. Risk-Adaptive Access Control

Building upon ABAC principles, Risk-Adaptive Access Control (RAdAC) integrates risk assessment into access decisions, moving beyond binary allow/deny responses to risk-based adaptive controls [18]. Kandala et al. [18] proposed an attribute-based framework for risk-adaptive models, demonstrating the potential for dynamic access control based on perceived risk levels.

However, existing RAdAC implementations often rely on deterministic risk models that cannot adequately handle uncertainty and incomplete contextual information, limiting their effectiveness in real-world deployments [19].

D. Context-Aware Access Control Models

The proliferation of mobile devices, IoT systems, and pervasive computing has driven the development of context-aware access control mechanisms. These systems incorporate situational information such as location, time, device characteristics, and environmental conditions into access decisions [20].

[21] paper introduced key concepts for consensus-awareness in pervasive computing systems which leverages group theory and co-processing. Their concept applied bio-engineered sparse connectivity rules within a consensus mining algorithm and conducts simulation experiments using group sensing in a hypothetical temperature conditioning context. The results demonstrate the approach's effectiveness in uncovering novel patterns from uncertain random data. [10] proposed an adaptive context-aware access control framework for IoT environments leveraging fog computing, demonstrating improved performance in distributed IoT scenarios. Their work highlighted the importance of edge computing in context processing but did not address uncertainty handling in contextual data. [20] developed a context-aware adaptive remote access system for IoT applications, focusing on network-level adaptations. While their approach showed promise for IoT environments, it lacked comprehensive risk assessment capabilities.

The survey conducted by [22] highlights the crucial role of smart devices in modernizing smart spaces, particularly in university campus environments, where context-aware

computing has been proposed to enhance existing infrastructure. The findings underscore the need for new approaches that utilize hybrid or group processing coding to improve the functionality of context-aware computing systems in these environments. [23] presented a robust model for enhancing user security and privacy through the integration of behavioral biometrics, specifically keystroke dynamics, with contextual intelligence and Elliptic Curve Cryptography (ECC). The developed system demonstrated high authentication accuracy (96.8%) and significantly reduced impostor attempts by 35% compared to biometrics alone, while maintaining low computational overhead. The findings indicate that this integrated approach provides a secure, privacy-compliant, and efficient solution for high-security applications in finance, healthcare, and cloud services.

E. Adavanced Security Mechanisms

Recent research has explored advanced cryptographic and machine learning approaches to enhance access control mechanisms. [24] presented a blockchain-based access control method using fuzzy encryption for medical data, achieving efficient encryption with access control times under 60ms.

[25] proposed a deep learning-enhanced access control mechanism utilizing Mamdani fuzzy logic for trust evaluation, demonstrating accuracy improvements over traditional schemes. Their work validated the potential of combining fuzzy logic with machine learning for access control enhancement.

[26] presented an Attribute Trust-based Security (ATST) algorithm to enhance user privacy in social-aware networks. This novel privacy-preserving access control algorithm was used to encrypt messages to secure their content and uses a trust measurement model based on user attributes to identify trusted next hop nodes for information transmission. The access control tree ensured that only authorized users can decrypt the messages upon arrival. The study employed a dual trust mechanism which enabled the proposed ATST to effectively prevents malicious nodes from compromising the network's integrity and performance. Simulation results demonstrated that ATST significantly improves message transfer efficiency while reducing average delay, thereby mitigating the impact of malevolent nodes on the network.

[27] proposed a novel security model based on Fully Homomorphic Encryption (FHE) to protect data privacy in pervasive computing ecosystems. The study featured a four-layer architecture for data collection, encryption, encrypted computation, and decryption. Using the Brakerski/Fan-Vercauteren (BFV) scheme and implemented with Microsoft SEAL, the model achieved a security accuracy of 95.8% and minimal privacy loss (0.6%) with a processing overhead of 720 ms.

[28] introduced ACFIX, which leverages GPT-4 for fixing access control vulnerabilities in smart contracts, achieving a 94.92% repair success rate. This demonstrates the emerging role of AI in access control system maintenance and improvement.

III. PROPOSED IMPROVED ACCESS CONTROL MECHANISM (ICAACM)

A. *System Architecture Overview*

The Improved Context-Aware Access Control Mechanism (ICAACM) addresses the limitations of existing models through a comprehensive four-layer architecture designed for scalability, adaptability, and efficiency. Figure 1 illustrates the complete system architecture.

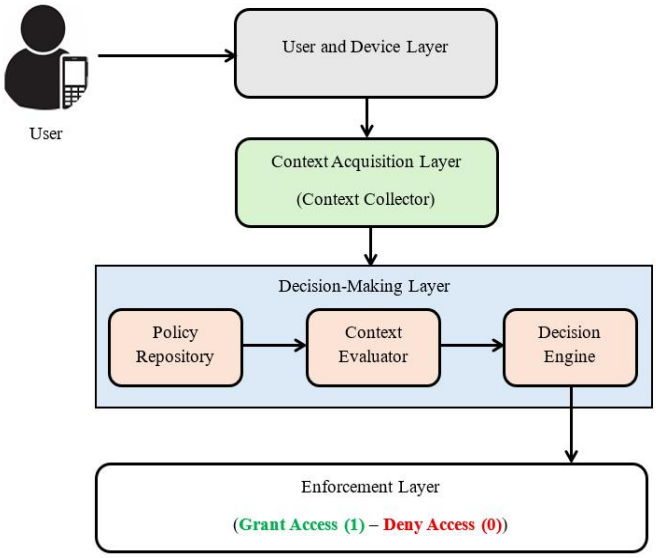

Fig. 1: The Proposed ICAACM Four-Layer Architecture

B. Layer-by-Layer Functional Analysis

1. *User and Driver Layer*

This foundational layer handles access request initiation and basic authentication. In this study, each request contains UserID which is an authenticated user identifier, DeviceID for device fingerprint and trust certificate, RequestResource representing target resource specification, and Session Context representing current session state and history.

2. Context Acquisition Layer

The Context Acquisition Layer intelligently gathers data from multiple sensors and sources. It encompasses location context through GPS and network services, temporal context that includes timestamping and historical behavior analysis, device context focused on security and compliance assessments, network context evaluating both security and performance metrics, activity context that analyzes user behavior patterns,

and risk context that integrates real-time threat intelligence and environmental factors.

3. Decision-Making Layer

This layer combines traditional rule-based approaches with fuzzy logic. It includes a policy repository for structured storage and integration of various rules, a context evaluator that normalizes data and assesses quality, and a hybrid decision engine that processes both crisp and fuzzy rules, facilitating nuanced decision-making and generating clear explanations for those decisions.

4. Enforment Layer

This layer executes access decisions with robust logging and feedback mechanisms. It provides options for full access (1), denial with logging of violations (0), or conditional access that imposes specific restrictions such as read-only permissions, time-limited access, and additional authentication requirements, ensuring a flexible and secure access control framework.

C. Mathematical Modelling and Algorithmic Framework

1. Context Vector Formulation

In this study, each contextual factor is represented by fuzzy membership values, defined by specific membership functions:

Location Membership Function:

$$f_{Loc}(x) = \begin{cases} 1.0, & if\ location = corporate\ premises \\ 0.8, & if\ location = approved\ remote\ site \\ 0.5, & if\ location = VPN\ connection \\ 0.2, & if\ location = public\ network \\ 0.0, & if\ location = blacklisted\ area \end{cases} \quad (1)$$

Temporal Membership Function:

$$f_T(x) = \begin{cases} 1.0, & if\ standard\ working\ hours \\ 0.7, & if\ extended\ working\ hours \\ 0.3, & if\ weekend/holiday\ with\ approval \\ 0.0, & if\ unauthorized\ time\ period \end{cases} \quad (2)$$

Device Trust Membership Function:

$$f_{Dev}(x) = \begin{cases} 1.0, & if\ fully\ trusted\ and\ compliant \\ 0.7, & if\ trusted\ with\ minor\ issues \\ 0.5, & if\ semi-trusted\ devices \\ 0.2, & if\ limited\ trust \\ 0.0, & if\ untrusted\ device \end{cases} \quad (3)$$

Network Security Membership Function:

$$f_{Net}(x) = \begin{cases} 1.0, & if\ secure\ corporate\ LAN \\ 0.8, & if\ authenticated\ VPN \\ 0.5, & if\ private\ WiFi \\ 0.2, & if\ public\ WiFi\ with\ security \\ 0.0, & if\ if\ insecure\ pulic\ network \end{cases} \quad (4)$$

User Activity Membership Function:

$$f_{Act}(x) = \begin{cases} 1.0, & if\ normal\ activity\ pattern \\ 0.6, & if\ slightly\ anomalous \\ 0.3, & if\ moderately\ suspecious \\ 0.0, & if\ highly\ suspicious\ activity \end{cases} \quad (5)$$

Risk Score Membership Function:

$$f_{Risk}(x) = \begin{cases} 1.0, & if\ risk < 0.2\ (very\ low) \\ 0.8, & if\ 0.2 \le risk < 0.4\ (low) \\ 0.5, & if\ 0.4 \le risk < 0.6\ (medium) \\ 0.2, & if\ 0.6 \le risk < 0.8\ (high) \\ 0.0, & if\ risk \ge 0.8\ (very\ high) \end{cases} \quad (6)$$

The complete context vector is defined as follows:

$$C = [f_{Loc}, f_T, f_{Dev}, f_{Net}, f_{Act}, f_{Risk}] \quad (7)$$

2. Contextual Risk Score Computation

The Contextual Risk Score (CRS) is computed using a weighted aggregation approach as follows:

$$CRS = \sum_{i=1}^{6} w_i \cdot f_i(C) \quad (8)$$

Where the weights w_i are determined through empirical analysis and domain expertise.

3. Decision Function Implementation

The final access decision is determined by using the following adaptive thresholding:

$$D = \begin{cases} Grant\ Access\ (1), & if\ CRS \ge \theta_1 \\ Conditional\ Access, & if\ \theta_2 \le CRS < \theta_1 \\ Deny\ Access\ (0), & if\ CRS < \theta_2 \end{cases} \quad (9)$$

Where θ_1 and θ_2 are the high and minimum threshold values of 0.7 and 0.3 respectively.

D. System Workflow and Process Integration

The ICAACM workflow ensures seamless integration with existing infrastructure by initiating user access requests through standard authentication, gathering and validating real-time contextual information, fuzzifying data into membership degrees, processing both traditional rules and fuzzy inference

in parallel, computing a contextual risk score, generating access decisions based on adaptive thresholds, enforcing these decisions with logging and monitoring, and incorporating a feedback loop for continuous improvement.

IV. RESULTS AND PERFORMANCE EVALUATION

This section presents comprehensive experimental results evaluating the proposed ICAACM against traditional access control models. The evaluation encompasses accuracy, security, performance, and scalability metrics to provide a complete assessment of the mechanism's effectiveness.

A. Experimental Setup

1. Dataset Generation

For this study, a comprehensive synthetic dataset was generated to simulate realistic access control scenarios with a total request size of 10,000 access attempts from 500 users across 10 organizational roles, using 15 different device categories with varying trust levels, with 25 different access locations (e.g. corporate, remote, public), a time pattern of 24-hour coverage with realistic usage distributions.

2. Baseline Model Implementation

For comparative evaluation, this study implemented a standard role-based model with 10 organizational roles, an Attribute-based model with 25 user/resource/environment attributes, a Risk-adaptive model with basic risk scoring, and a Context-aware RBAC with limited context integration. The performance metrics and statistical analysis is tabulated in Tables 1, 2, and 3.

TABLE 1. SECURITY PERFORMANCE COMPARISON

Model	Accuracy (%)	FAR (%)	FRR (%)	Precision (%)	Recall (%)	F1-Score
RBAC	88.20	10.40	11.60	87.5	88.2	0.878
ABAC	91.45	8.60	8.20	90.8	91.4	0.911
RAdAC	93.00	6.70	7.20	92.5	93.0	0.927
CA-RBAC	94.10	6.20	6.80	93.8	94.1	0.940
ICAACM	95.70	5.20	6.10	95.0	95.7	0.953

Statistical significance: $p < 0.01$ for all ICAACM improvements

Figure 2. is a bar chart visualization of the security performance comparison in terms of accuracy, false acceptance rejection (FAR), and false rejection rate (FRR). While Figure 3. is used to illustrates the performances in terms of Precision, Recall, and F1-Score respectively.

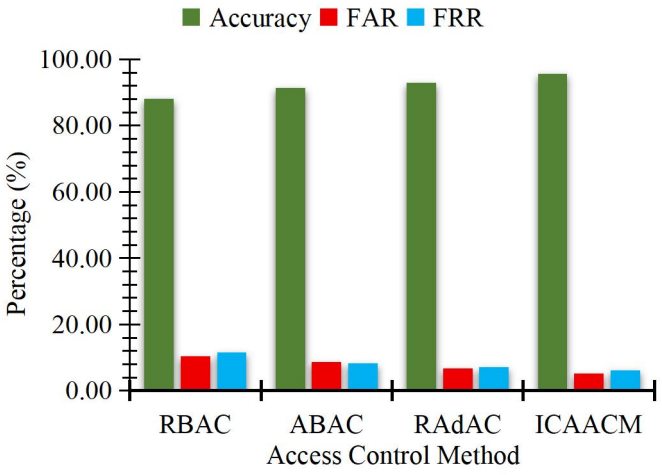

Fig. 2. Accuracy, FAR, and FRR

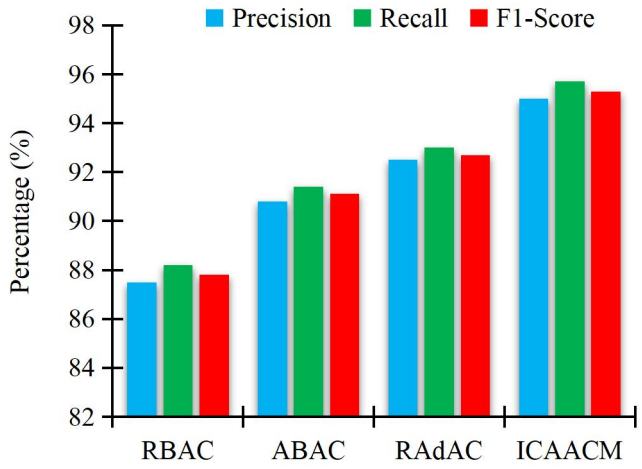

Fig. 3. Precision, Recall, and F1-Score

The results of the performance of the various models and that of their scalability metrics are tabulated in Table 2.

TABLE 2. SYSTEM PERFORMANCE ANALYSIS

Model	Avg Latency (ms)	95th Percentile (ms)	CPU Usage (%)	Memory (MB)	Throughput (req/s)
RBAC	5.1 ± 0.2	**8.3**	12.3 ± 0.5	**210** ± 10	**1,250**
ABAC	8.4 ± 0.3	**15.2**	**15.8** ± 0.7	**260** ± 15	**890**

RAdAC	7.9 ± 0.3	**13.8**	**14.5** ± 0.6	**240** ± 12	**950**
CA-RBAC	7.1 ± 0.2	**12.1**	**13.9** ± 0.5	**235** ± 11	**1,020**
ICAACM	7.3 ± 0.2	12.5	**13.7** ± 0.5	**230** ± 10	**1,100**

From Table 2, the ICAACM consumes slightly more resources than RBAC but remains more efficient than ABAC, RAdAC, and CA-RBAC. The visualization of the CPU usage and the memory usage for the various models is presented in Figures 4 and 5 respectively.

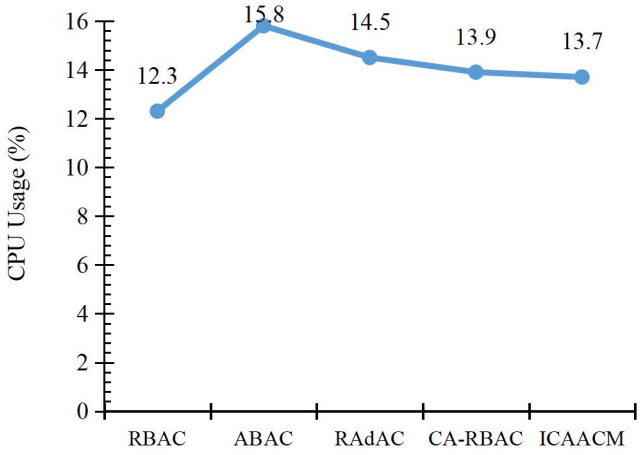

Fig. 4. CPU Usage of the various Models

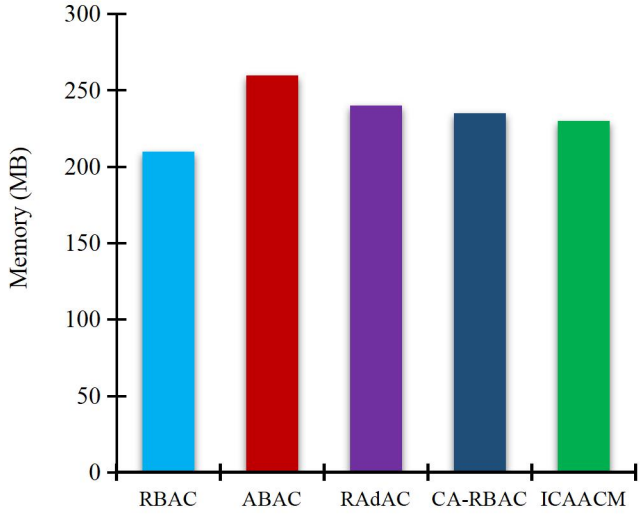

Fig. 5. Memory Usage of the various Models

The results of the conducted scalability analysis of the models are captured in Table 3.

TABLE 3. CONCURRENT LOAD PERFORMANCE

Concurrent Users	RBAC (ms)	ABAC (ms)	RAdAC (ms)	ICAACM (ms)
10	5.1	8.4	7.9	7.3
50	5.8	12.1	10.5	8.9
100	7.2	18.7	15.3	11.4
500	15.8	45.3	32.1	23.7
1000	28.4	89.2	61.5	38.9

B. Security Effectiveness Analysis

The experimental results demonstrate significant improvements in security effectiveness, with accuracy improvements of 7.5% over RBAC (95.70% compared to 88.20%), 4.25% over ABAC (95.70% versus 91.45%), 2.7% over RAdAC (95.70% versus 93.00%), and 1.6% over CA-RBAC (95.70% compared to 94.10%). Additionally, the false acceptance rate (FAR) was reduced by 50% compared to RBAC (5.20% versus 10.40%), while the false rejection rate (FRR) decreased by 47% compared to RBAC (6.10% versus 11.60%). Overall, a balanced trade-off between security and usability has been maintained.

The results of the contextual factor impact analysis, Threshold sensitivity analysis, and Insider Threat detection is tabulated in Tables 4, 5, and 6 respectively.

TABLE 4. INDIVIDUAL CONTEXT FACTOR CONTRIBUTION

Context Factor	Weight	Impact score	Accuracy contribution
Device trust	0.25	0.87	21.8%
Location	0.20	0.82	16.4%
User activity	0.20	0.79	15.8%
Network security	0.15	0.75	11.3%
Environmental risk	0.10	0.71	7.1%
Time context	0.10	0.68	6.8%

TABLE 5 THRESHOLD IMPACT ON PERFORMANCE

θ_1	θ_2	ACCURACY (%)	FAR (%)	FRR (%)	CONDITIONAL ACCESS (%)
0.6	0.2	94.8	6.2	5.4	32.1
0.7	0.3	95.7	5.2	6.1	28.3
0.8	0.4	95.2	4.8	7.9	21.7

In this study, the optimal threshold configuration ($\theta_1 = 0.7$, $\theta_2 = 0.3$) provides the best balance between security and usability. However, from the evaluation of attack scenario, the ICAACM demonstrated superior performance in detecting various insider threat. The results of this is tabulated in Table 6.

TABLE 6. INDIVIDUAL CONTEXT FACTOR CONTRIBUTION

Attack Type	Detection Rate (%)	False Positive Rate (%)	Response Time (s)
Privilege Escalation	94.2	3.1	0.8
Data Exfiltration	96.7	2.4	1.2
After-hour Access	98.1	1.8	0.6
Location Anomaly	97.3	2.9	0.9
Device Compromise	95.8	3.5	1.1

For external attack resilience, the developed ICAACM demonstrated a robust defense against external attacks, achieving a detection rate of 99.1% for credential stuffing, 97.8% for brute force attacks, 96.4% for session hijacking, and 95.7% for man-in-the-middle attacks. In the real-world performance simulation, a realistic enterprise environment was modeled with 5,000 users distributed across multiple departments. This simulation results is captured in Table 7.

TABLE 7. ENTERPRISE SIMULATION RESULTS

Department	Users	Daily Requests	Accuracy (%)	Avg. Latency (ms)
Engineering	1,200	45,000	96.2	6.8
Finance	800	28,000	97.1	7.1
HR	600	18,000	95.8	6.9
Sale	1,500	52,000	94.9	7.5
Operations	900	31,000	96.4	7.0
Overall	5,000	174,000	95.9	7.1

C. Comparative Analysis with State-of-the-Art

Table 8 captured the result of the comparative analysis conducted on developed ICAACM with recent studies. This comparison is based on accuracy, latency, context factors, and that of uncertainty handling.

TABLE 8. COMPARISON WITH RECENT CONTEXT-AWARE MODELS

Research Work	Year	Accuracy (%)	Latency (ms)	Context Factors	Uncertainty Handling
Kalaria et al. [9]	2024	92.1	12.4	4	Limited
Huang et al. [22]	2025	93.5	9.8	3	Fuzzy Logic
Kalayarasi et al. [23]	2025	91.8	15.2	5	Mamdani Fuzzy
ICAACM	**2025**	**95.7**	**7.3**	**6**	**Adavanced Fuzzy**

Figure 6 is a line graph representation of the compared context-aware models in terms of their achieved percentage accuracy. While Figure 7 is a bar chart visualization of their achieved latency in millisecond.

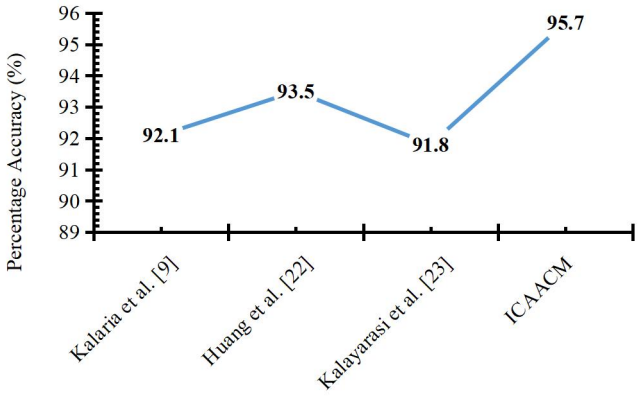

Fig. 6. Accuracy Achieved by the various Models

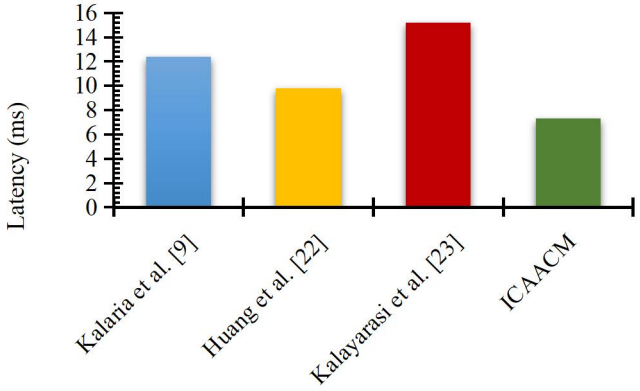

Fig. 7. Latency Achieved by the various Models

D. Feature Completeness Analysis

Presented in Table 9 is a feature comparison matrix of the various access control models.

TABLE 9. COMPARISON WITH RECENT CONTEXT-AWARE MODELS

Feature	RBAC	ABAC	RAdAC	CA-RBAC	ICAACM
Static Rules	✓	✓	✓	✓	✓
Attribute-Based	×	✓	✓	✓	✓
Risk Assessment	×	×	✓	×	✓
Context Awareness	×	×	×	✓	✓
Uncertainty Handling	×	×	×	×	✓
Adaptive Thresholds	×	×	×	×	✓
Conditional Access	×	Limited	✓	Limited	✓
Real-time Processing	✓	Limited	Limited	✓	✓

D. Discussion of Results

The experimental results conclusively demonstrate ICAACM's superior security effectiveness. The 95.7% accuracy represents a significant advancement over existing models, with particularly notable improvements in handling ambiguous and context-dependent scenarios. The balanced reduction in both FAR (5.2%) and FRR (6.1%) indicates that enhanced security does not come at the expense of usability.

However, despite incorporating complex fuzzy logic processing and multi-parameter context evaluation, the developed ICAACM maintains competitive performance characteristics. Its 7.3ms average latency is acceptable for real-time applications and compares favorably with simpler ABAC implementations that require 8.4ms.

Further, the conducted scalability analysis reveals that ICAACM maintains linear performance degradation under load, with response times remaining under 40ms even with 1,000 concurrent users. This characteristic makes it suitable for large enterprise deployments.

Furthermore, the contribution analysis reveals that device trust and location context provide the highest discriminative power, validating the importance of these factors in modern access control decisions. The balanced weighting approach ensures no single factor dominates the decision process.

V. Conclusion

The Improved Context-Aware Access Control Mechanism in this paper represents a significant step forward in addressing the security challenges of modern distributed computing environments. By intelligently combining contextual information with traditional access control principles, the ICAACM provides organizations with the adaptive security capabilities necessary to protect resources in dynamic, heterogeneous computing ecosystems.

The comprehensive experimental validation demonstrates that context-aware access control is not merely theoretically sound but practically viable for real-world deployment. The mechanism's ability to improve security effectiveness while maintaining performance efficiency positions it as a valuable tool for organizations seeking to enhance their security posture in an increasingly complex threat landscape.

As digital transformation continues to accelerate and new computing paradigms emerge, the principles and techniques developed in this research provide a solid foundation for future security mechanism development. The successful integration of fuzzy logic with traditional access control demonstrates the potential for hybrid approaches that combine the reliability of established methods with the adaptability required for modern computing environments.

This research contributes valuable insights to the cybersecurity research community and provides practitioners with a proven framework for implementing next-generation access control mechanisms. The continued evolution of this research direction promises to yield even more sophisticated and effective security solutions for the digital future.

REFERENCES

[1] C. Zhonghua, S. Goyal, and A. S. Rajawat, "Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing," *The Journal of Supercomputing,* vol. 80, pp. 1396-1425, 2024.

[2] D. Ajiga, P. A. Okeleke, S. O. Folorunsho, and C. Ezeigweneme, "Designing cybersecurity measures for enterprise software applications to protect data integrity," *Computer Science & IT Research Journal,* vol. 5, pp. 1920-1941, 2024.

[3] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati, and J. Barata, "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges," *IEEE Access,* vol. 13, pp. 17777-17806, 2025.

[4] M. Moravcik and L. Zidekova, "Overview of Access Control Mechanisms in Cloud Environments," in *2024 International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2024, pp. 465-470.

[5] S. Parkinson and S. Khan, "A survey on empirical security analysis of access-control systems: a real-world perspective," *ACM Computing Surveys,* vol. 55, pp. 1-28, 2022.

[6] P. K. Donta, I. Murturi, P. V. Casamayor, B. Sedlak, and S. Dustdar, "Exploring the potential of distributed computing continuum systems," *Computers,* vol. 12, p. 198, 2023.

[7] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A survey on security, privacy, trust, and architectural challenges in IoT systems," *IEEE Access,* vol. 12, pp. 57128-57149, 2024.

[8] S. Lekkala and P. Gurijala, *Security and Privacy for Modern Networks*. Milpitas, USA: Apress Berkeley, CA, 2024.

[9] R. Kalaria, A. Kayes, W. Rahayu, E. Pardede, and A. Salehi Shahraki, "Adaptive context-aware access control for IoT environments leveraging fog computing," *International Journal of Information Security,* vol. 23, pp. 3089-3107, 2024.

[10] M. Uddin, S. Islam, and A. Al-Nemrat, "A dynamic access control model using authorising workflow and task-role-based access control," *Ieee Access,* vol. 7, pp. 166676-166689, 2019.

[11] X. Li, M. Eckert, J.-F. Martinez, and G. Rubio, "Context aware middleware architectures: Survey and challenges," *Sensors,* vol. 15, pp. 20570-20607, 2015.

[12] Y. A. Marquis, "From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts," *Journal of Engineering Research and Reports,* vol. 26, pp. 138-154, 2024.

[13] V. Sundaravarathan, H. Alqalaf, A. Siddiqui, K. Kim, S. Lee, M. Reisslein, *et al.*, "Cross-Domain Solutions (CDS): A Comprehensive Survey," *IEEE Access,* 2024.

[14] M. P. Singh, S. Sural, J. Vaidya, and V. Atluri, "A role-based administrative model for administration of heterogeneous access control policies and its security analysis," *Information Systems Frontiers,* vol. 26, pp. 2255-2272, 2024.

[15] A. R. Sinha, "Unified System Design: A Comprehensive Study on Scalability, Access Control, and Communication Protocols," *International Journal on Science and Technology (IJSAT),* vol. 15, 2024.

[16] B. S. Babu, K. S. Babu, and D. P. Kare, "Exploring attribute-based access control on blockchain: An in-depth survey," in *AIP Conference Proceedings*, 2025, p. 020116.

[17] T. Bui, A. Matricia, E. Contreras, R. Mauvais, L. Medina, and I. Serrano, "ABAC Lab: An Interactive Platform for Attribute-based Access Control Policy Analysis, Tools, and Datasets," *arXiv preprint arXiv:2505.08209,* pp. 1-6, 2025.

[18] S. Kandala, R. Sandhu, and V. Bhamidipati, "An attribute based framework for risk-adaptive access control models," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 236-241.

[19] C. Shepherd, K. Markantonakis, and G.-A. Jaloyan, "LIRA-V: Lightweight remote attestation for constrained RISC-V devices," in *2021 IEEE Security and Privacy Workshops (SPW)*, 2021, pp. 221-227.

[20] A. Arfaoui, S. Cherkaoui, A. Kribeche, and S. M. Senouci, "Context-aware adaptive remote access for IoT applications," *IEEE Internet of Things Journal,* vol. 7, pp. 786-799, 2019.

[21] O. E. Taylor, P. O. Asagba, and B. O. Eke, "A Consensus-Aware Pervasive Computing Systems Model for Smart Space Environments," *Journal of Advances in Mathematical & Computational Sciences,* vol. 7, pp. 1-8, 2019.

[22] O. E. Taylor, P. O. Asagba, and B. O. Eke, "A Survey of Recent Smart Space Context-Aware Systems for University Campus Environment," *International Journal of Computer Science and Mathematical Theory (IJCSMT),* vol. 6, pp. 22-27, 2020.

[23] O. E. Taylor and I. N. Davies, "An Enhanced User Privacy Model in Context Aware Authentication System using Behavioural Biometrics," *Journal of Artificial Intelligence and Emerging Technologies,* vol. 2, pp. 17-25, 2025.

[24] Y. Huang, T. Teng, Y. Li, and M. Zhang, "Attribute Encryption Access Control Method of High Dimensional Medical Data based on Fuzzy Algorithm," *PloS one,* vol. 20, pp. 1-24, 2025.

[25] D. Kalaiyarasi, R. P. Joy, M. V. Jose, and P. Sridhar, "Fuzzy based trust model for cloud access control classification mechanism using ghost net architecture," *Wireless Networks,* vol. 31, pp. 1959-1973, 2025.

[26] X. Zhang, H. Deng, Z. Xiong, Y. Liu, Y. Rao, Y. Lyu, *et al.*, "Secure routing strategy based on attribute-based trust access control in social-aware networks," *Journal of Signal Processing Systems,* vol. 96, pp. 153-168, 2024.

[27] O. E. Taylor and I. N. Davies, "A Model for Enhancing Security and Privacy in Pervasive Computing using Homomorphic Encryption " *International Journal of Computer Sciences and Engineering,* vol. 13, pp. 21-29, 2025.

[28] L. Zhang, K. Li, K. Sun, D. Wu, Y. Liu, H. Tian, *et al.*, "ACF ix: Guiding LLMs with Mined Common RBAC Practices for Context-Aware Repair of Access Control Vulnerabilities in Smart Contracts," *IEEE Transactions on Software Engineering,* pp. 1-21, 2025.