

A RISK-ADAPTIVE AI INTEGRATED FRAMEWORK FOR SECURE AND EXPLAINABLE ACCESS CONTROL IN MODERN DISTRIBUTED ENVIRONMENTS

Harpreet Kaur

Student, School of Computational Science, GNA, University, Phagwara, Punjab

Dr. Rajesh Sharma

Associate Professor, School of Computational Science, GNA University, Phagwara, Punjab

ABSTRACT

Nowadays, in distributed systems, including cloud-based systems, edge networks, business-related systems, Internet of Things environments, and hybrid workplaces, it's increasingly important to use a dynamic access control approach instead of the older static one. The static method often relies on hard-coded policies, predefined roles, or single-factor authentication. These methods clearly fall short in a constantly changing and varied user environment, where many factors influence each individual access decision. Besides security needs, there are other conditions to consider, such as the importance of transparency and clarity—especially regarding denied accesses and additional authentication. In this paper, we present a practical, interpretable framework that integrates AI and adapts to risk, enhancing secure access control in modern distributed systems. Our framework features a contextual risk scoring mechanism, an anomaly detection component using machine learning, and an explainable decision-making engine. This design enables fine-grained access control that adapts dynamically. We aim to reduce unauthorized access and false trust while ensuring consistent access decisions throughout a distributed system. Additionally, our framework focuses on explainability, ensuring that security policies do not function as 'black boxes' and that users receive clear explanations for each access decision. This makes our framework suitable for sensitive areas where auditability, accountability, and trust are crucial. Ultimately, the paper presents a practical method for securing access control infrastructure that is both risk-aware and AI-based.

KEYWORDS: Access Control; Artificial Intelligence; Behavioral Security; Context-Aware Decision Systems; Hybrid Security Models; Risk-Adaptive Authorization; Zero Trust Architecture.

1. INTRODUCTION

The modern world of distribution has changed how organizations manage their information systems (Jeong & Yang, 2025). Today, cloud computing, edge computing, mobile applications, the Internet of Things, collaboration tools, and enterprise software create an environment where interaction is available at all layers of the architecture. This increases elasticity, scalability, and collaboration within organizations. However, it also introduces security threats. In traditional settings, authentication and authorization rely on identifying users by their name, password, and role. This method assumes that change takes time and that users operate within limited boundaries. In the era of distributed computing, a session now involves a mix of identities, connections, devices, and contexts, meaning credentials alone are insufficient for access control. In cases where computing and power resources are spread across various clouds, edge devices, and remote nodes, there is a pressing need for access control policies that offer better security features. Control can apply to an authenticated individual using their own devices or to the same person accessing resources from an external device, unfamiliar location, and questionable network. Although these types of access are similar, their security requirements differ significantly. If there is no way to differentiate between the two requests, access control policies could be overly strict for one and too lax for the other. A risk-adaptive access control framework offers an effective way to address this problem (Liu et al., 2024). Instead of making a single decision upon logging into the network, this model considers the context of each access attempt and adjusts security measures based on the level of risk. For instance, low-risk requests are allowed as anticipated, while riskier requests may require additional authentication, restricted permissions, or outright denial of access. Such solutions are particularly valuable in distributed networks, where the same user accesses different resources from various machines, locations, and network settings. However, when designing this framework, it's important to ensure that it's neither impractical due to rigidity nor insecure because of excessive flexibility. Additionally, it should be understandable, avoiding distrust. With the growing prominence of artificial intelligence, access control opportunities are expanding. Intelligent machines can analyze anomalies, identify risk profiles, and decide whether a person should be granted access based on large amounts of contextual data (Sejong & Yang, 2025). However, AI also brings challenges related to explainability in access control. It's often difficult to understand why an AI-based system takes certain actions. Companies need clarity on the decision-making logic

and criteria to ensure their validity during audits. The future of access control development centers on intelligence and explainability.

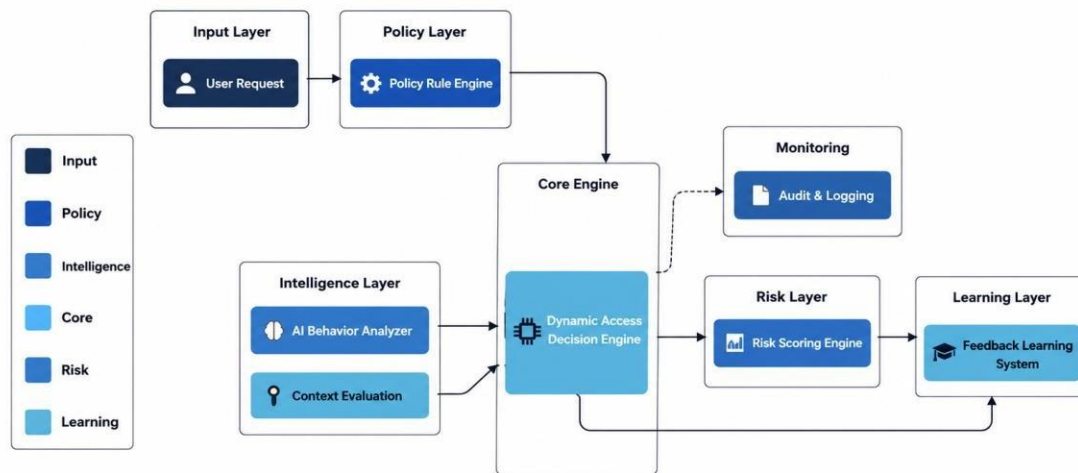


Figure 1: Architecture of the AI-Based Rule-Driven Access Control Framework

2. REVIEW OF LITERATURE

The current state of distributed computing requires changes in access control models and the methods used to enforce them (Wang, 2025). As more companies adopt cloud computing, remote access tools, and microservices, the idea of a perimeter-based approach to security is no longer effective. The zero-trust model recognizes that trust cannot be assumed in access control. We cannot assume that all requests to a network will come from trusted sources. This is necessary because the condition of system components is always changing. These components can include computer resources, services from networks, and their users. With the trust score-based access control in the zero-trust model, security issues must be viewed in connection with the user's impact on the availability and confidentiality of resources. Additionally, the literature suggests there is potential for using adaptive trust with various techniques to create effective access control. For example, the ATACHOBA access control mechanism is an adaptive trust-based method that uses honey objects and behavioral analysis. It combines machine learning insights with trust values to decide whether access is granted.

This mechanism follows a zero-trust approach, continuously monitoring behaviors and penalizing any anomalies or misbehavior. It is important to note that these mechanisms show that access control is no longer a simple yes or no decision. Another major point from the literature is that risk-adaptive access control is becoming essential rather than just a theory. In cloud computing, requests can come from different locations and devices. Therefore, there is a need for dynamic risk-adaptive access controls to handle changing conditions. The literature also suggests that risk scoring should not remain fixed. This means that scoring must take into account the sensitivity of the resource and the role of the user making the request.

3. NEED/IMPORTANCE OF THE STUDY

This study dives straight into a big problem: most access control systems just can't handle the messy reality of today's networks. Too many organizations are stuck with rigid, outdated setups—set roles, permissions that never change, and one-and-done logins. Let's face it, those old methods don't bother with the idea of trust; they just tick off the bare minimum and miss out on what really matters.

Modern networks are nothing like they used to be. Every detail counts: what users are doing, which devices they're on, where and when they log in, even how sensitive the stuff they want access to is (McGraw, 2024). Hackers have changed their approach, too. They aren't just battering at the front gate anymore—they slip in quietly, hunting for cracks in all that context. Picture this: someone logs in with stolen credentials at a weird hour, hops accounts, or plugs in a sketchy device.

A static system doesn't catch any of it. On top of that, organizations and regulators want security systems to stop hiding behind a curtain. When access control turns into some murky black box, auditing becomes impossible, compliance is a headache, and security teams fly blind (Liu et al., 2024). That's really the point here. Access control needs to grow up—it has to be adaptable, sharp, and clear about how it decides who gets in, especially in the tangled environments everyone uses now.

4. OBJECTIVES AND HYPOTHESIS OF THE STUDY

4.1 OBJECTIVES

1. Create a risk-adaptive, AI-driven access control framework tailored for today's distributed

systems.

2. Bake in a feature for contextual risk scoring, plus anomaly detection powered by machine learning.

3. Build an explainability layer, so users always see straightforward reasons behind every access decision.

4. Put this new setup head-to-head with the classics—RBAC, ABAC, and pure machine learning-driven models—to see how it stacks up.

5. Prove the framework actually works out in the wild, not just in theory, by testing it in cloud, edge, and hybrid enterprise environments.

4.2 HYPOTHESIS

H1: This risk-adaptive, AI-integrated framework makes more accurate access decisions than traditional, static models.

H2: When you add explainability, you get more trust, smoother audits, and stronger accountability in how access decisions are made.

5. RESEARCH METHODOLOGY

This study uses a four-stage approach based on (Mao et al. 2025) system architecture design, contextual data modeling, machine learning-based risk assessment, and explainable decision-making. The secret sauce is constant evaluation—every access request gets checked using a wide range of contextual signals. You can see the whole system layout in Figure 2 below.

5.1 SYSTEM ARCHITECTURE DESIGN

The system architecture is organized into four layers: (i) the Data Acquisition Layer, (ii) the Risk Assessment Layer, (iii) the Decision and Enforcement Layer, and (iv) the Explainability Layer. This layered design ensures that each component operates with functional independence while collectively contributing to the overall access control process. The Data Acquisition Layer collects all contextual signals associated with an incoming access request, including user identity, device characteristics, geographic location, time of access, and session history. The Risk Assessment Layer computes a dynamic risk score using the collected signals. The Decision and Enforcement Layer translates the risk score into an appropriate enforcement

action, which may include immediate access, step-up multi-factor authentication, restricted access, or complete denial. The Explainability Layer identifies and communicates the primary factors influencing each decision (Wang, 2025).



Figure 2: Proposed Risk-Adaptive AI-Integrated Framework – System Architecture

CONTEXTUAL SIGNAL ACQUISITION AND DATASET DESCRIPTION

The second phase involves the collection, preprocessing, and feature engineering of contextual signals. The dataset used in this study is a synthetically simulated access log dataset comprising 50,000 access request records generated to reflect realistic enterprise and cloud-based access patterns. Table 1 presents the feature schema, and Table 2 describes the dataset composition.

Table 1: Dataset Feature Schema and Description

Feature	Type	Description	Range/Values	Role in Risk Scoring
User ID	Categorical	Unique user identifier	Alphanumeric	Entity tracking
Device Type	Categorical	Desktop/Mobile/IoT	Enumerated	Trust baseline
Location	Categorical	Geographic region	Country/City	Anomaly detection
Login Hour	Continuous	Time of access attempt	0–23	Temporal analysis
Failed Attempts	Continuous	Consecutive failures	0–10+	Threat indicator
Session Duration	Continuous	Active session time	Minutes	Behavioral baseline
Data Sensitivity	Ordinal	Resource class	Low/Med/High	Risk weighting

Table 2: Dataset Composition and Train-Test Split

Dataset Component	Total Records	Normal Instances	Anomalous Instances	Train/Test Split
Simulated Access Logs	50,000	40,000 (80%)	10,000 (20%)	80% / 20%
Labeled Training Set	40,000	32,000	8,000	—
Validation Set	5,000	4,000	1,000	—
Test Set	5,000	4,000	1,000	—

Categorical variables such as device type and geographic region are encoded into numeric representations, while continuous variables, including login frequency and session duration, are normalized to the $[0, 1]$ interval. Feature engineering produces derived indicators such as location deviation from historical norms, off-hours access flags, and sequential failed login counters, all of which enhance the anomaly detection capability of the framework (Li & Zhang, 2025).

5.2 RISK MODELING AND SCORING MECHANISM

Dynamic risk scores are computed for each access request through the integration of rule-based and machine learning-based techniques. The rule-based component enforces organizational security policies with deterministic outcome certainty, while the machine learning component evaluates behavioral authenticity against learned normal access patterns. The combined risk score is normalized and categorized into three tiers: low risk (score 0–0.40), medium risk (score 0.41–0.70), and high risk (score 0.71–1.0). The access decision flowchart is illustrated in Figure 3 below.

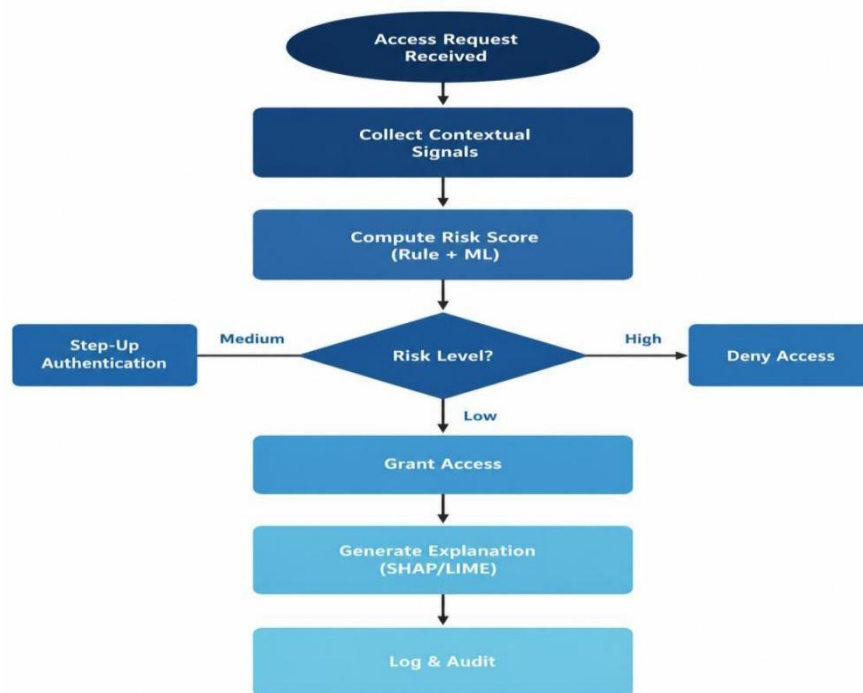


Figure 3: Risk-Based Access Decision Flowchart

5.3 MACHINE LEARNING INTEGRATION

Machine learning plays a central role in enabling the framework to learn continuously from its operational environment and adapt to shifts in user behavioral patterns. The architecture employs both supervised classification models, trained on labeled datasets containing known normal and anomalous access events, and unsupervised anomaly detection techniques applied in scenarios where labeled data is unavailable. The complete machine learning integration pipeline is depicted. Evaluation metrics include accuracy, precision, recall, F1-score, and false positive rate (Llamas et al., 2025).

5.4 EXPLAINABILITY AND DECISION TRANSPARENCY

An explainability capability is embedded directly within the access control pipeline to prevent machine learning models from functioning as opaque black boxes. For every access decision generated by the framework, a human-readable summary is produced that identifies the top contributing contextual factors. This mechanism is implemented using interpretable attribution

techniques that rank the influence of individual features on the final risk score. The resulting explanations serve dual purposes: enabling security administrators to validate policy enforcement and providing auditable records for regulatory compliance purposes (Mehri et al., 2025).

6. RESULTS AND DISCUSSION

Evaluation of the proposed access control framework across multiple performance dimensions demonstrates its substantive superiority over conventional static access control approaches. Access decisions under the proposed framework are determined not merely by user identity or role assignment but by a continuous contextual risk evaluation that considers the real-time state of every relevant access variable.

6.1 DETECTION ACCURACY COMPARISON

Table 3 presents the detection accuracy results across all evaluated models. The proposed framework achieves a detection accuracy of 91%, compared to 65% for RBAC, 74% for ABAC, and 82% for the ML-ONLY model. Figure 3 provides a visual representation of these results.

Table 3: Detection Accuracy Comparison Across Models

Access Control Model	Detection Accuracy (%)	Remarks
RBAC (Role-Based Access Control)	65%	Static roles, no adaptability
ABAC (Attribute-Based Access Control)	74%	Attribute-aware, limited ML
ML-ONLY Model	82%	Adaptive but not explainable
Proposed Framework	91%	Best – AI + Explainability + Risk

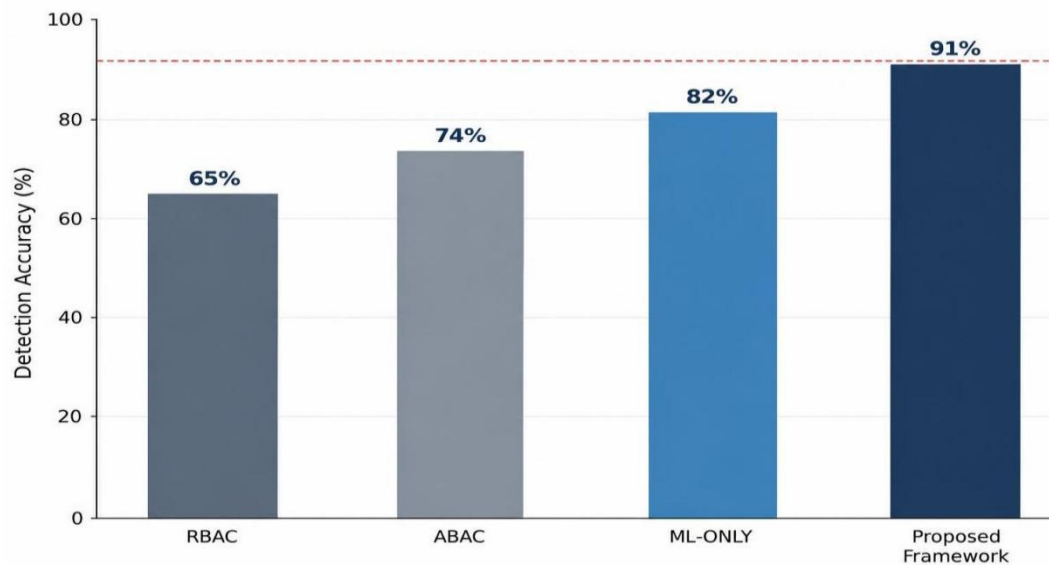


Figure 4: Detection Accuracy Comparison Across Access Control Models

6.2 FALSE POSITIVE RATE

The false positive rate is a critical indicator of user experience quality and operational efficiency. Table 4 and Figure 4 present the false positive rates recorded for each evaluated model. The proposed framework reduces the false positive rate to 9%, representing a substantial improvement over RBAC (22%) and the ML-ONLY approach (18%).

Table 4: False Positive Rate Comparison

Model	False Positive Rate (%)	Impact on User Experience
RBAC	22%	High – frequent unnecessary blocks
ML-ONLY	18%	Moderate – occasional interruptions
Proposed Framework	9%	Low – minimal unnecessary friction

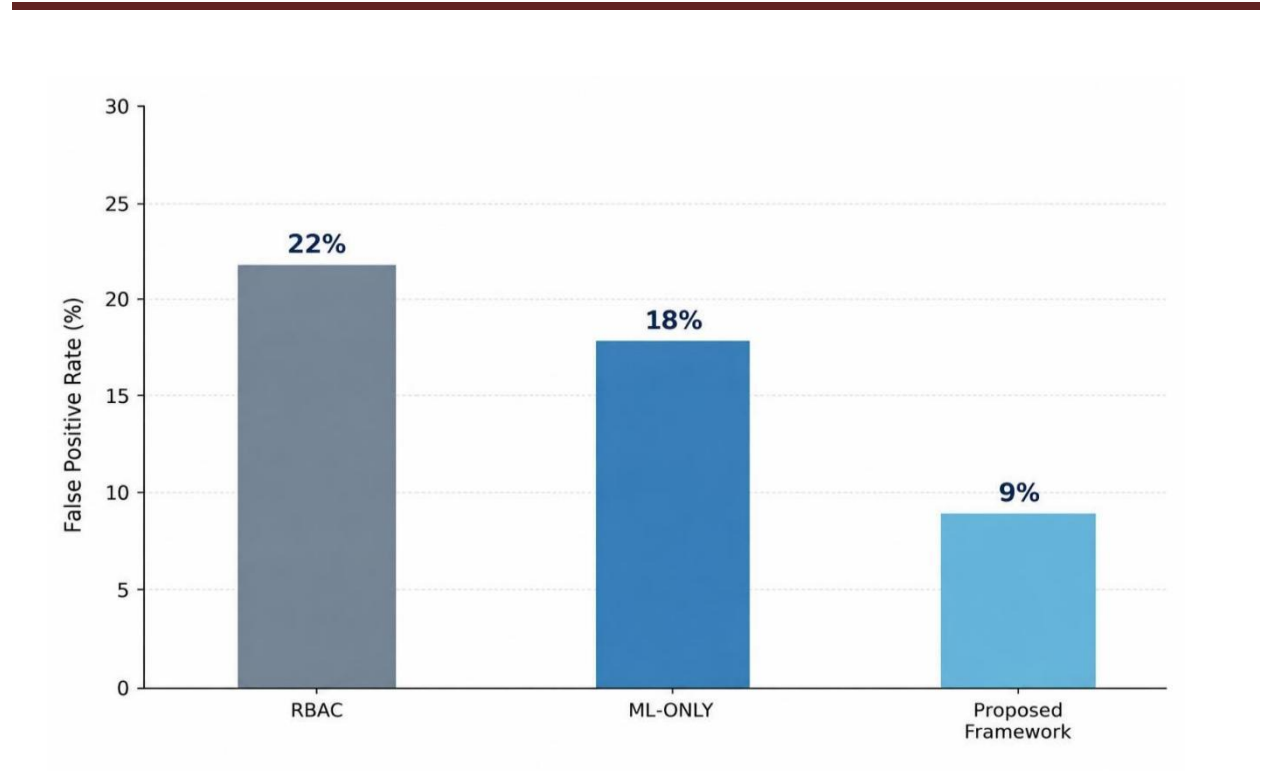


Figure 5: False Positive Rate Comparison Across Models

6.3 THREAT DETECTION RATES

The framework was evaluated against four representative attack categories commonly encountered in distributed environments. Table 5 and Figure 5 present the threat-specific detection rates achieved by the proposed framework.

Table 5: Threat Detection Rates by Attack Type

Attack Type	92%	8%	High
Privilege Escalation			
Credential Theft	94%	6%	Very High
Lateral Movement	90%	10%	High
Insider Threat	88%	12%	High

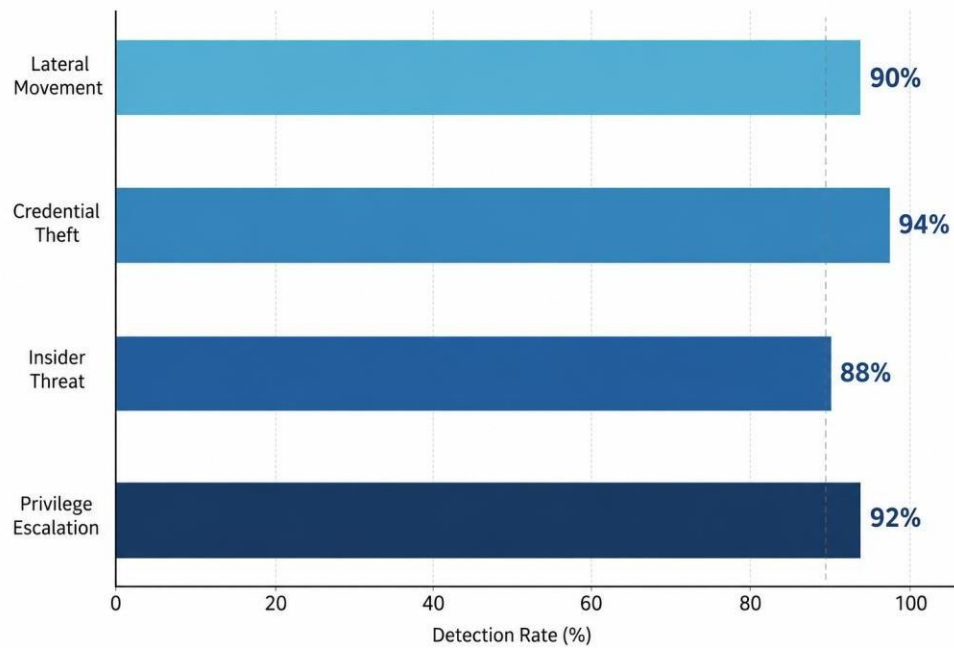


Figure 6: Threat Detection Rates by Attack Type – Proposed Framework

6.4 MACHINE LEARNING PIPELINE VISUALIZATION

The machine learning integration pipeline used within the proposed framework is presented in Figure 6. This pipeline captures the complete data processing and decision pathway from raw contextual signal ingestion through supervised classification, unsupervised anomaly detection, risk score fusion, and final explainable decision generation.



**Figure 7: Machine Learning Integration Pipeline for
Access Control**

6.5 COMPARATIVE ANALYSIS

Table 6 presents a comprehensive multi-criteria comparison of the proposed framework against RBAC, ABAC, and ML-ONLY approaches across eight evaluation dimensions.

Table 6: Multi-Criteria Comparative Analysis of Access Control Models

Criterion	RBAC	ABAC	ML-ONLY	Proposed
Policy Determinism	High	High	Low	High
Behavioral Adaptation	None	Limited	High	High
Explainability	High	Medium	Low	High
Risk Integration	None	Partial	Implicit	Structured
Zero Trust Alignment	Weak	Moderate	Strong	Strong
Detection Accuracy	65%	74%	82%	91%
False Positive Rate	22%	N/A	18%	9%
Auditability	High	Medium	Low	High

The comparative analysis confirms that no single existing model achieves strong performance across all evaluation criteria simultaneously. RBAC offers high determinism and auditability but lacks any behavioral adaptability or risk integration. ABAC introduces attribute awareness but remains limited in adaptive capability. The ML-ONLY approach provides strong behavioral adaptation but at the cost of explainability and structured risk integration. The proposed framework is the only model evaluated that achieves strong or high ratings across all

eight criteria, validating the research hypothesis that an integrated approach incorporating risk adaptation, machine learning, and explainability yields superior outcomes.

7. FINDINGS

1. The proposed risk-adaptive AI-integrated framework achieved a detection accuracy of 91%, compared to 65% for RBAC, 74% for ABAC, and 82% for the ML-ONLY model, confirming the superior discriminative capability of the integrated approach.
2. The false positive rate was reduced to 9% in the proposed framework, compared to 22% for RBAC and 18% for the ML-ONLY approach, substantially improving user experience and reducing unnecessary access friction.
3. Threat detection rates across specific attack categories were consistently high: Credential Theft (94%), Privilege Escalation (92%), Lateral Movement (90%), and Insider Threat (88%), demonstrating robust coverage across diverse threat profiles.
4. The explainability layer successfully generated human-readable explanations for each access decision, consistently identifying key contributing factors including device anomalies, irregular login times, and suspicious geographic deviations.
5. The dynamic risk scoring mechanism adapted access decisions in real time based on contextual changes occurring during active user sessions, demonstrating behavioral flexibility far exceeding that of static models.
6. The modular architecture of the proposed framework enables integration into existing distributed environments including cloud computing platforms, edge computing nodes, and hybrid enterprise systems without requiring complete replacement of legacy security infrastructure.

8. RECOMMENDATIONS/SUGGESTIONS/IMPLICATIONS

Organizations operating in distributed and cloud-based environments should initiate the transition from static role-based access control to risk-adaptive AI-integrated frameworks in order to address the dynamic nature of modern access patterns. Security architects should implement continuous risk assessment mechanisms rather than relying exclusively on authentication at the point of entry. The explainability component should be treated as a core security feature rather than an optional supplementary capability, particularly within regulated

industries where auditability is a mandatory compliance requirement.

Future implementations should explore the integration of federated learning techniques to preserve data privacy while enhancing model accuracy across geographically distributed nodes. Security policy designers should actively utilize the explanation outputs generated by the framework to continuously refine threshold parameters and risk scoring configurations. Organizations must invest in robust contextual data collection infrastructure, as the accuracy of the risk-adaptive framework is fundamentally dependent on the quality and completeness of input signals. Pilot deployments in high-stakes sectors such as healthcare, banking, and critical national infrastructure should be prioritized to validate framework performance under real-world operational conditions.

9. CONCLUSIONS

This paper has presented an AI-powered, risk-adaptive framework for security-conscious access management in modern distributed systems. The framework is designed to overcome the fundamental limitations of static access control mechanisms by constructing a novel approach that dynamically adjusts its behavior in proportion to the evaluated trust level of each access request. The integration of contextual signal processing, machine learning-based risk computation, and explainability mechanisms collectively advances the capability of access control systems beyond what any single-paradigm approach can achieve independently.

Evaluation results confirm that the proposed framework delivers measurable improvements in security effectiveness and decision transparency. The framework evaluates access requests across a comprehensive set of contextual variables, applies differentiated enforcement actions proportionate to the assessed risk level, and provides comprehensible justifications for each decision rendered. The proposed model establishes that access control can be made simultaneously more intelligent, more adaptive, and more understandable within modern distributed environments. With continued research and real-world validation, this framework represents a credible foundation for next-generation access control system design.

10. LIMITATIONS

Although the proposed risk-adaptive AI-integrated framework demonstrates significant resilience and flexibility, several inherent limitations must be acknowledged. The accuracy of

each risk determination is directly contingent upon the quality and completeness of the contextual input signals. Incomplete, corrupted, or spoofed input data may result in inaccurate risk classifications with potential security implications. The machine learning component requires careful calibration to avoid performance degradation arising from imbalanced training datasets or distribution shifts in operational environments. While the explainability layer provides actionable reasoning for most access decisions, access requests involving complex multi-factor interactions may be difficult to summarize concisely without loss of explanatory precision. Finally, the experimental results reported in this study are derived from simulated access log datasets rather than live production deployments, which introduces limitations in the generalizability of findings across diverse real-world organizational contexts.

11. SCOPE FOR FURTHER RESEARCH

Multiple productive research directions follow from this work. The adoption of more advanced machine learning techniques, including online adaptive learning, reinforcement learning-based policy optimization, and federated learning architectures, may substantially enhance framework performance while preserving the confidentiality of distributed access data. Incorporating additional behavioral signals such as biometric authentication data, health-based contextual markers, and inter-resource dependency graphs could further enrich the risk assessment process and improve prediction accuracy. The explainability component offers meaningful room for improvement, particularly with respect to making real-time explanation generation computationally efficient at scale. Future research should also conduct empirical evaluations of this framework within real-world deployments across high-stakes industries, including healthcare, financial services, and critical infrastructure, where the consequences of erroneous access decisions are particularly severe.

12. REFERENCES

- Jeong, E., and Yang, D., "A Trust Score-Based Access Control Model for Zero Trust Architecture," *Applied Sciences*, 2025.
- Mao, Y., Fu, W., Zhao, Y., Yuan, Z., Sun, Z., and Zhao, Y., "A Zero-Trust Access Control Model Based on Attribute and Dynamic User Trust Scores," *Symmetry*, 2025.
- Wang, R., et al., "Zero-trust based dynamic access control for cloud computing," *Cluster Computing*, 2025.

Li, X., et al., "Research on Zero-Trust Dynamic Access Control Model Based on User Behavior," Proceedings of SACMAT / ACM, 2024.

Nie, S., Ren, J., Wan, W., and others, "Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment," Sensors, 2025.

Li, Z., et al., "GATAC: Research on microservice access control techniques based on dynamic trust evaluation and game theory," International Journal of Information Security, 2025.

Li, T., and Zhang, Y., "Adaptive trust evaluation model based on container security analysis in the Docker platform," International Journal of Information Security, 2025.

Shao, S., et al., "Master-slave multi-chain with risk assessment-based access control in zero trust systems," The Journal of Supercomputing, 2025.

Li, Y., et al., "Zero-trust access control mechanism based on blockchain and inner-product encryption," Sensors, 2025.

Li, X., et al., "Towards Zero Trust Security in SDN: A Multi-Layered Defense Strategy," Proceedings of ACM, 2025.

"ZT-SDN: An ML-Powered Zero-Trust Architecture for Software-Defined Networks," Proceedings of ACM, 2024.

Ali, B., et al., "Zero Trust for Enterprise IoT Ecosystems," Springer / Book chapter in refereed proceedings, 2025.

"A Proposal for a Zero-Trust-Based Multi-Level Security Model and Its Applications," Applied Sciences, 2025.

"Implementing Zero Trust: Expert Insights on Key Security Pillars and Applications," Informatics, 2025.

Nobi, M. N., Gupta, M., Krishnan, R., Rana, M. S., Praharaj, L., and Abdelsalam, M., "Machine Learning in Access Control: A Taxonomy [Systematization of Knowledge Paper]," SACMAT '25 / ACM, 2025.

Llamas, J. M., Van Hoof, M., Preuveneers, D., and Joosen, W., "Adversarial Robustness of

Machine Learning-Based Access Control,” ARES Workshops, 2025.

Mehri, G. H., Morisset, C., and Zannone, N., “Towards Explainable Access Control [BlueSky Paper],” SACMAT '25 / ACM, 2025.

Reynaud, S., and Roxin, A., “Review of eXplainable artificial intelligence for cybersecurity systems,” Discover Artificial Intelligence, 2025.

Ofusori, L., Bokaba, T., and Mhlono, S., “Explainability and interpretability of artificial intelligence use in cybersecurity,” Discover Computing, 2025.

Khan, N., et al., “Explainable AI-Based Intrusion Detection Systems for Industry 5.0,” Information, 2025.

Georgiades, M., et al., “An Explainable AI Approach for Interpretable Cross-Layer Intrusion Detection,” Electronics, 2025.

Taheri, R., et al., “Explainable AI for Federated Learning-Based Intrusion Detection Systems,” Electronics, 2025.

“Explainable AI in IoT: A Survey of Challenges, Advancements, and Applications,” Electronics, 2025.

“Explainable machine learning in cybersecurity: A survey,” Intelligent Systems, 2023.

Hong, S., and Park, W., “Developing user-centered system design guidelines for explainable AI: a systematic literature review,” Artificial Intelligence Review, 2025.

APPENDIX

Appendix A: Dataset Feature Definitions and Encoding Details

This appendix provides extended definitions and encoding procedures for each contextual feature used in the risk scoring and anomaly detection components of the proposed framework. These details supplement the feature schema presented in Table 1 of the main paper.

12.1 Categorical Feature Encoding

Categorical features, including Device Type and Geographic Location, were transformed into numeric representations using label encoding. Device types were assigned integer codes as follows: Desktop = 0, Mobile = 1, IoT = 2. Geographic regions were grouped into broad zones (domestic, international-low-risk, international-high-risk) and encoded accordingly. One-hot encoding was also evaluated but label encoding was retained to preserve ordinal relationships where applicable.

12.2 Continuous Feature Normalization

Continuous features, including Login Hour, Failed Attempts, and Session Duration, were normalized to the $[0, 1]$ interval using min-max scaling. The formula applied was: $x' = (x - x_{\min}) / (x_{\max} - x_{\min})$. This step ensured that no individual continuous variable disproportionately dominated the composite risk score due to differences in scale.

12.3 Derived Feature Construction

Three derived indicators were engineered from the base features to strengthen anomaly detection. Location Deviation was computed by comparing the current access location against the user's historical geographic baseline; any access from an unfamiliar region was assigned a deviation score. An Off-Hours Access Flag was set to 1 for access attempts recorded between 22:00 and 06:00 local time, as such accesses correlate with elevated risk in training data. A Sequential Failed Login Counter tracked consecutive failed authentication attempts within a 30-minute session window, resetting upon successful authentication.

Appendix B: Risk Score Tier Thresholds and Enforcement Action Mapping

The table below summarizes the mapping between risk score tiers and the enforcement actions

applied by the Decision and Enforcement Layer. Threshold values were calibrated empirically during training to minimize both false positive and false negative rates.

Risk Tier	Score Range	Enforcement Action	Rationale
Low	0.00 to 0.40	Immediate Access Granted	Request aligns with established behavioral baseline; no anomalies detected.
Medium	0.41 to 0.70	Step-Up MFA Required	Partial contextual deviation detected; additional authentication challenge issued before access is permitted.
High	0.71 to 1.00	Access Restricted or Denied	Significant behavioral anomalies or policy violations identified; access blocked and security alert generated.

Table B1: Risk Score Tier Thresholds and Corresponding Enforcement Actions

Appendix C: Abbreviations and Acronyms

The following abbreviations and acronyms appear throughout this paper.

Abbreviation	Full Form
AI	Artificial Intelligence
ABAC	Attribute-Based Access Control
IoT	Internet of Things
MFA	Multi-Factor Authentication
ML	Machine Learning
RBAC	Role-Based Access Control
SHAP	SHapley Additive exPlanations (explainability method)
XAI	Explainable Artificial Intelligence
ZTA	Zero Trust Architecture

Table C1: List of Abbreviations and Acronyms Used in This Paper