OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Identity-Centric Security Models for Enterprise Web Systems

Md Ariful Islam[1]*, Farhan Tariq[2], Mabu Hussain Shaik[3], Shujath Baig Mirza[4]

[1]MSC in Computer Science and Engineering Jagannath University, Bangladesh
[2]Department of Software Engineering, University- University of Gujrat, Sialkot Campus, Pakistan
[3]Master of Science in Information Technology Management University- Campbellsville University, KY, United States
[4]Master of Science in Engineering Management University- Saint Martin's University, Lacey, Washington

DOI: https://doi.org/10.36348/sjet.2026.v11i04.008 | **Received:** 11.02.2026 | **Accepted:** 06.04.2026 | **Published:** 11.04.2026

***Corresponding author:** Md Ariful Islam
MSC in Computer Science and Engineering Jagannath University, Bangladesh

Abstract

Enterprise web systems support many organizational functions, including digital transactions, cloud services, data storage, and enterprise software operations. As these systems operate across distributed infrastructures, traditional security models based on static authentication and network boundaries face significant limitations. This study proposes an identity-centric security model that integrates identity authentication, identity profiling, behavioral monitoring, risk evaluation, and policy-based access control within a unified framework. The model evaluates identity activity continuously during active sessions instead of relying only on initial login verification. Identity profiles contain contextual information derived from authentication attributes, device information, location data, and historical usage patterns. Behavioral monitoring observes session activity and identifies deviations from established patterns. A risk evaluation mechanism combines authentication irregularities and behavioral deviations to calculate identity risk scores. These scores guide policy-based access decisions within enterprise applications. Experimental analysis using simulated enterprise session data indicates improved anomaly detection capability, faster response to suspicious activity, and higher accuracy in access decisions compared with traditional role-based access control systems. Continuous monitoring and adaptive policy evaluation allow enterprise platforms to react to changing identity conditions during system interaction. The findings indicate that identity-centric security frameworks provide a context-aware approach for protecting enterprise web systems.

Keywords: Identity-Centric Security, Enterprise Web Systems, Identity and Access Management (IAM), Behavioral Monitoring, Identity Risk Evaluation, Adaptive Access Control, Enterprise Cybersecurity, Risk-Based Authentication, Access Control Models, Enterprise Security Architecture.

I. INTRODUCTION

Enterprise web systems support a wide range of organizational activities, including digital transactions, data management, cloud services, and enterprise software platforms. These systems operate across distributed infrastructures that include cloud environments, enterprise networks, and third-party integrations. The emergence of web-based enterprise applications has created a situation of increased risk in terms of security breaches. Unauthenticated access, the exploitation of credentials, and identity theft are common security breaches in web-based applications. Traditional security practices are based on network boundaries and perimeter security. However, such practices are not effective in distributed systems, as applications and services are deployed on multiple platforms. The Identity and Access Management (IAM) system is a security practice that governs the security of the authentication and authorization process in the enterprise. The IAM system manages the identity of users and provides access control to the applications. A systematic review of IAM requirements reports growing demand for identity governance systems capable of supporting complex organizational structures and cross domain identity verification [10]. Decentralized identity models such as self-sovereign identity also appear in current research as alternatives to centralized identity management frameworks.

Enterprise infrastructures present additional challenges for identity governance. Modern web systems connect multiple services that include APIs, enterprise databases, cloud platforms, and external applications.

Access control policies must function consistently across these systems while maintaining reliable identity verification processes. Research on integrated access control models proposes architectures that combine organizational roles with entity-level identity structures for enterprise authorization control [17]. Such models address hierarchical permission structures within organizations. However, enterprise environments continue to face difficulties related to identity lifecycle control, policy administration, and detection of abnormal authentication activity. Cloud computing platforms have become an important component of enterprise web infrastructure. Many organizations rely on hybrid architectures that integrate on-premise systems with cloud services. Research on disaster recovery and high-availability architectures examines system continuity and service availability within hybrid cloud environments [3]. Secure data management frameworks also address protection of enterprise datasets during digital transformation initiatives in financial and information technology systems [2]. The infrastructure monitoring tools offer additional operational insights through analytics-based dashboards for resource utilization and infrastructure performance across various distributed computing infrastructures. However, research in infrastructure development focuses on these areas with minimal emphasis on identity-based security mechanisms. Emerging technologies also influence enterprise cybersecurity research. Blockchain-based access control systems record authentication and authorization activities in distributed ledgers that maintain immutable records of access events [7]. Such systems provide mechanisms for decentralized verification of digital identities. Federated learning frameworks allow multiple organizations to conduct collaborative data analysis without sharing raw datasets, which supports secure inter-agency cooperation in critical infrastructure sectors [1]. Artificial intelligence also appears in enterprise security architectures. AI-driven IoT security systems combine cloud computing and blockchain platforms to detect threats in connected infrastructures [12]. Research also proposes blockchain-secured communication mechanisms for industrial IoT networks and aviation control platforms [13].

Cybersecurity monitoring systems contribute additional protection within enterprise environments. Vulnerability management and automated incident response frameworks analyze system activity and identify security weaknesses in corporate networks [6]. Research on IoT-based electric vehicle ecosystems examines authentication risks, privacy concerns, and communication security challenges within connected transportation infrastructures [4]. Industrial automation environments present similar cybersecurity requirements. A smart SCADA framework integrates cloud computing, industrial IoT technologies, and cybersecurity mechanisms within industrial control systems [15]. Edge computing architectures also support distributed computing infrastructures used in energy and transportation networks [11]. Enterprise cybersecurity research also addresses financial monitoring and governance systems. Financial risk intelligence platforms analyze transaction activity and detect abnormal financial patterns in enterprise systems [9]. Ethical data governance frameworks examine responsible data management and artificial intelligence accountability in enterprise information systems [14]. Disaster recovery automation systems support hybrid cloud infrastructures through automated backup and restoration mechanisms that maintain system continuity during operational disruptions [16]. The research conducted in infrastructure development, infrastructure security, infrastructure monitoring systems, and infrastructure-based access control mechanisms have shown these areas as isolated domains of research. However, in distributed enterprise web systems, it is necessary to develop a security model with identity verification mechanisms, access control mechanisms, and cybersecurity monitoring systems under a single umbrella.

This study proposes an identity-centric security model for enterprise web systems that integrates identity governance, access control mechanisms, and cybersecurity monitoring within distributed enterprise architectures. The research aims to address limitations in current enterprise security frameworks and support consistent identity management across enterprise web platforms.

II. Related Work

A. Identity and Access Management in Enterprise Systems

Identity and Access Management (IAM) governs authentication, authorization, and identity control in enterprise web systems. Organizations deploy IAM platforms to regulate user access across applications, databases, and digital services. A systematic review of enterprise IAM requirements reports the need for scalable identity governance and decentralized identity models such as self-sovereign identity [10]. The study notes challenges associated with identity federation, cross-domain authentication, and management of extensive organizational identity records. Research also examines access control models developed for enterprise platforms. An integrated access control model that combines organizational roles with entity-level identity relationships addresses complex authorization structures in enterprise systems [17]. The model introduces hierarchical policy structures that regulate permissions across organizational units. Additional work evaluates monitoring techniques in cloud-based IAM environments. Real-time anomaly detection systems analyze authentication logs and identify irregular login behavior and access attempts [8]. These studies demonstrate progress in IAM technologies; however, issues related to identity lifecycle management and large-scale policy administration remain.

B. Cloud Infrastructure Security and Data Management

Enterprise web platforms often operate in hybrid cloud infrastructures that combine private and public computing resources. Disaster recovery research examines methods that maintain service availability and data continuity across distributed cloud environments [3]. Hybrid recovery architectures support enterprise operations during infrastructure failures and system outages. Enterprise systems also require secure data management strategies. Research on scalable data management frameworks addresses protection of enterprise datasets while supporting digital transformation initiatives within finance and information systems [2]. These frameworks consider data storage security, access monitoring, and governance policies across enterprise databases. Infrastructure monitoring tools also support enterprise operations. Resource utilization analytics dashboards monitor system performance and track cloud infrastructure activity across distributed platforms [18]. Despite these developments, many infrastructure security studies focus primarily on system performance and operational management, while identity centered protection receives limited discussion.

C. Emerging Security Technologies in Enterprise Protection

Recent studies investigate advanced technologies such as blockchain, artificial intelligence, and federated learning for cybersecurity applications. Blockchain-based access control systems record authentication events and authorization transactions in decentralized ledgers [7]. Distributed ledgers provide immutable records of access activities and support verification of digital identities within cloud environments. Federated learning has also appeared in collaborative security research. A federated learning framework allows multiple organizations in critical infrastructure sectors to perform joint data analysis without transferring raw datasets across institutions [1]. The architecture supports distributed machine learning while preserving data confidentiality. Artificial intelligence also appears in enterprise cybersecurity systems. AI-powered IoT security architectures combine blockchain and cloud platforms for threat detection in connected infrastructures [12]. Research also presents blockchain-secured communication mechanisms for industrial IoT networks and aviation control systems [13]. These technologies introduce new approaches to cybersecurity; however, integration with identity governance models in enterprise web systems remains limited.

D. Cybersecurity Monitoring and Enterprise Risk Management

Cybersecurity monitoring systems support threat detection and vulnerability management in enterprise networks. Automated incident response frameworks monitor network activity and identify vulnerabilities across corporate systems [6]. These frameworks assist administrators in responding to security incidents and system threats. Other studies address cybersecurity issues in connected infrastructures and industrial platforms. Research on IoT-based electric vehicle ecosystems examines authentication risks, communication security, and privacy protection in connected transportation environments [4]. Industrial automation environments present similar challenges. A smart SCADA framework integrates cloud computing, industrial IoT technologies, and cybersecurity controls within industrial automation systems [15]. Edge computing architectures also appear in security research. Distributed edge frameworks support secure computing across energy and transportation infrastructures [11]. Enterprise security research also considers financial monitoring and governance frameworks. Financial risk intelligence platforms analyze transaction activity and identify abnormal financial patterns in digital systems [9]. Ethical data governance models examine responsible data management and AI accountability within enterprise information systems [14]. Disaster recovery automation in hybrid cloud environments supports system continuity and data recovery after infrastructure disruptions [16]. Despite these developments, research rarely presents identity-centered security architectures designed specifically for enterprise web systems.

Summary of Research Gap

Current research addresses IAM frameworks, hybrid cloud security, blockchain access control, AI-based cybersecurity systems, and enterprise monitoring platforms. These domains often appear as separate research areas. Few studies present unified architectures that combine identity governance, behavioral monitoring, and enterprise web application security. Research that integrates identity centered security models with distributed enterprise systems remains limited.

III. METHODOLOGY

This study introduces an identity centric security model designed for enterprise web systems that operate across distributed infrastructures. The proposed methodology integrates identity authentication, behavioral observation, risk evaluation, and policy-driven access control within a unified security framework. Conventional enterprise security architectures rely primarily on role-based access control (RBAC) and static authentication procedures. These processes check identity during the login process and rarely check identity activity during an active session. These weaknesses create opportunities for the abuse of credentials and unauthorized system access. The proposed model evaluates identity continuously throughout system interaction. Authentication verification, behavioral observation, and risk scoring operate together to determine access permissions. The methodology consists of five interconnected stages: identity data collection, identity profiling, behavioral

monitoring, identity risk assessment, and policy-based access control. Each stage contributes to a dynamic evaluation process that assesses identity trust levels during system operation.

A. System Architecture of the Identity-Centric Security Model

The architecture introduces several components responsible for identity verification and access management in enterprise web environments. These components include an authentication layer, identity profiling module, behavioral monitoring engine, risk evaluation unit, and policy enforcement mechanism. Enterprise applications interact with this security layer before access to protected resources occurs.

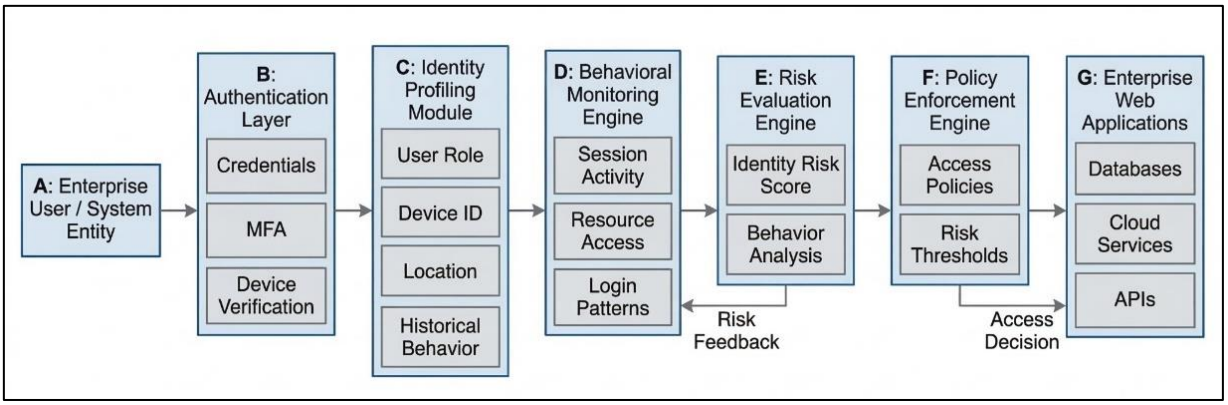

Figure 1: Proposed Identity-Centric Security Architecture

Figure 1 presents the structural design of the proposed model. The authentication layer checks identity credentials and authenticates other factors, such as user accounts, devices, and session context. Once authenticated, the system creates an identity profile with contextual information related to the user or system entity. The behavioral monitoring module records activity within enterprise applications. Observed events pass to the risk evaluation component, which calculates an identity risk score. A policy engine interprets this score and determines access permissions for enterprise resources. The architecture introduces continuous identity evaluation throughout the session. Behavioral analysis and risk scoring allow the system to reassess identity conditions during application interaction. This structure supports adaptive security decisions in enterprise web environments.

B. Data Collection and Identity Profiling

The first methodological stage involves collecting identity-related data from enterprise information systems. Data sources include authentication records, user account attributes, device identifiers, application activity logs, and network metadata. These datasets provide the foundation for constructing identity profiles. Identity profiling organizes collected information into structured identity attributes. Each profile contains details such as organizational role, authentication method, device type, geographic location, and historical usage patterns. Identity profiles represent contextual information associated with each enterprise user or system entity. Historical system activity contributes to behavioral baseline construction. A behavioral baseline represents typical patterns associated with identity activity. For example, a user who regularly accesses enterprise applications during specific working hours or from consistent network locations produces a predictable activity pattern. Deviations from these patterns signal possible security concerns. Identity profiling therefore supports contextual interpretation of behavioral activity within enterprise systems.

C. Behavioral Monitoring and Identity Risk Evaluation

Behavioral observation forms the analytical core of the proposed methodology. The system monitors user actions during enterprise application interaction. Examples include login frequency, resource access requests, session duration, and device switching patterns. These observations create behavioral indicators that reflect identity activity within enterprise environments.

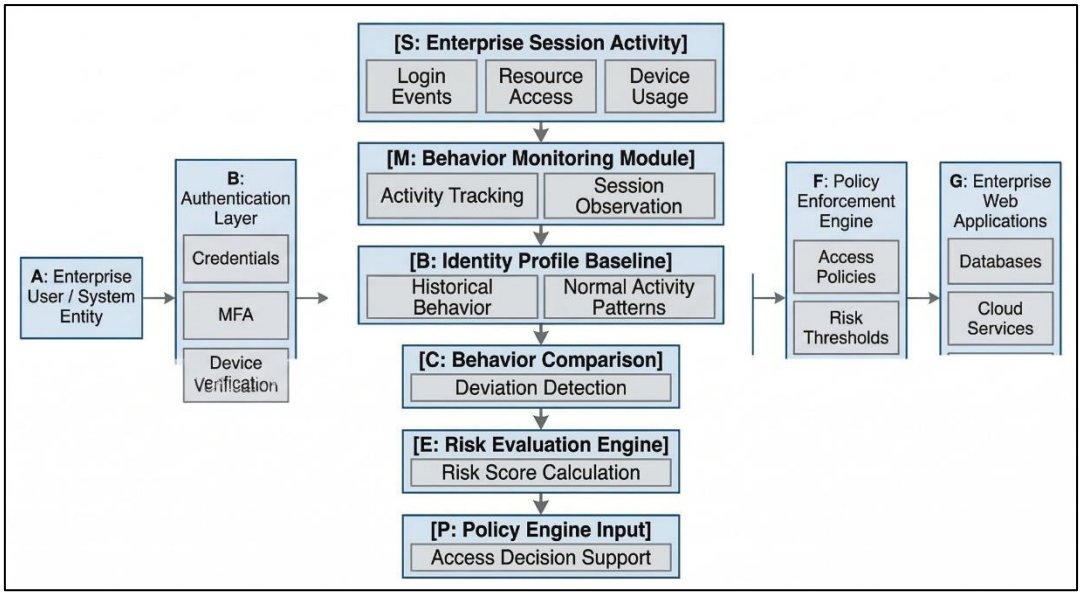

Figure 2: Identity Risk Evaluation and Behavior Analysis Workflow

Figure 2 illustrates the analytical process used to evaluate behavioral information and calculate identity risk. Behavioral indicators collected from enterprise applications undergo comparison with identity profile baselines. The system identifies deviations that differ from expected patterns.

An identity risk score represents the probability that observed activity indicates suspicious behavior. The study applies a simplified evaluation formula:

$R_i = \alpha A_i + \beta B_i$

where R_i represents the risk score assigned to identity i, A_i represents authentication-related risk factors, and Bi represents behavioral anomaly indicators. Parameters α and β represent weighting values that control the influence of authentication and behavioral elements. Higher risk scores appear when abnormal activity patterns occur. Examples include unfamiliar device usage, unusual geographic access, repeated authentication failures, or irregular system interaction sequences. Continuous monitoring allows risk values to change during the active session.

D. Policy-Based Access Control and Decision Process

The access decision mechanism interprets identity risk scores through policy evaluation. Enterprise security policies define acceptable risk thresholds associated with different user roles and system resources. The policy engine compares risk values with thresholds and determines access permissions.

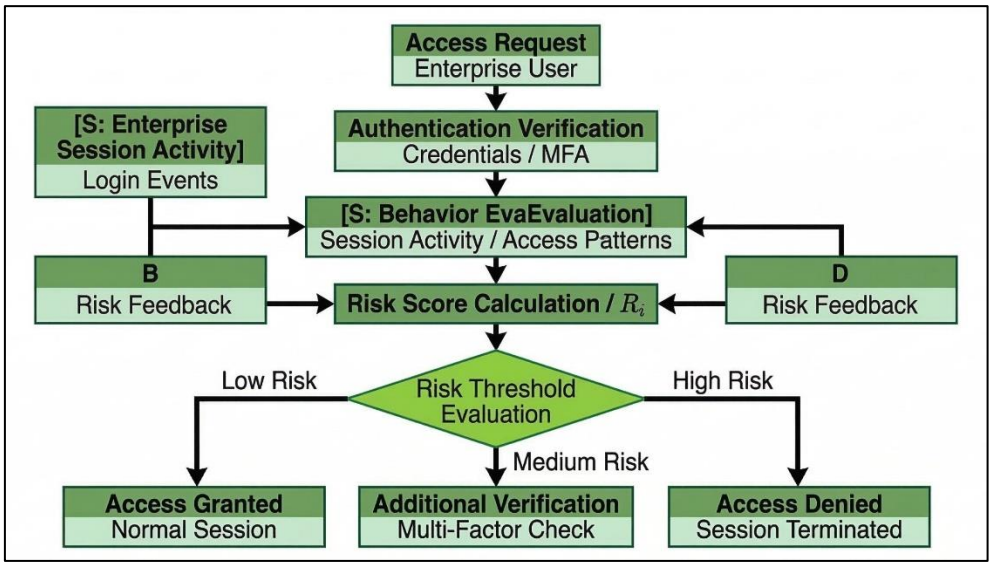

Figure 3: Access Decision Process in the Identity-Centric Security Model

Figure 3 illustrates the decision workflow used during an access request. Following authentication and behavioral evaluation, the calculated risk score enters the policy assessment stage. Access permission depends on

the resulting evaluation outcome. Low risk values allow access to enterprise services. Intermediate risk values trigger additional verification procedures such as multi-factor authentication. High risk values result in session termination or access denial. The decision model supports adaptive security control within enterprise web environments. Access policies respond to real-time identity conditions rather than relying solely on static user roles.

E. Core Components of the Proposed Identity-Centric Model

The primary elements of the proposed security framework appear in Table 1.

Table 1: Key Components of the Identity-Centric Security Model

Component	Description	Security Function
Authentication Factors	Credentials, device validation, multi-factor verification	Identity verification
Identity Attributes	User role, device information, location, account context	Identity profile creation
Behavioral Indicators	Login frequency, session activity, resource access patterns	Behavioral observation
Risk Evaluation Module	Compute's identity risk score using behavioral and authentication data	Threat probability evaluation
Policy Enforcement Engine	Applies enterprise policies to determine access permissions	Access decision management

F. Methodological Contribution

The methodology introduces an identity-centered evaluation process that differs from traditional RBAC frameworks. Conventional access control models depend on predefined roles and static authentication steps. The proposed approach evaluates identity conditions continuously during enterprise system interaction. Behavioral observation, risk scoring, and policy evaluation operate together to determine access permissions. This framework supports detection of credential misuse, abnormal identity behavior, and unauthorized access attempts within enterprise web systems. Continuous identity evaluation and adaptive policy interpretation provide stronger protection for distributed enterprise infrastructures.

IV. DISCUSSION AND RESULTS

This section evaluates the performance of the proposed identity-centric security model in enterprise web environments. The analysis follows the methodological framework introduced earlier, which includes identity profiling, behavioral monitoring, risk evaluation, and policy-based access control. The evaluation used simulated enterprise session logs containing authentication records, device information, access requests, and behavioral activity patterns. The results focus on three analytical aspects: identity behavior patterns, identity risk score distribution, and the effectiveness of policy-based access decisions. These results also provide a comparison between the proposed identity-centric model and traditional role-based access control (RBAC) systems. The analysis demonstrates how behavioral monitoring and risk-based evaluation support adaptive security decisions in enterprise environments.

A. Identity Behavior Analysis Results

Identity behavior analysis examines patterns of user activity during enterprise sessions. The behavioral monitoring module collected information related to login events, resource access frequency, device usage, and geographic access locations. Identity profiles created during earlier methodological stages provided reference baselines representing normal activity patterns for enterprise users. Results show that most enterprise sessions follow stable activity patterns. Employees typically access enterprise applications during consistent working hours and from predictable network locations. Device usage also tends to remain consistent across sessions. These patterns form the behavioral baseline used for identity evaluation. Certain sessions exhibited noticeable deviations from expected behavior. Examples include sudden device changes, login attempts from unfamiliar locations, and irregular resource access sequences. These deviations triggered anomaly indicators within the monitoring system. Behavioral indicators formed an important component of identity risk evaluation. The analysis also revealed differences between role-based permissions and behavioral activity patterns. Two users with identical role privileges may interact with enterprise systems in different ways. One user may access databases frequently, while another performs limited tasks within a specific application. Static access control models treat both identities similarly. Behavioral monitoring introduces additional context that allows the security system to evaluate activity patterns rather than relying solely on role assignments. These results confirm that behavioral analysis contributes valuable information for enterprise security evaluation. Continuous observation of identity activity allows detection of irregular patterns that static authentication systems cannot identify.

B. Risk Score Evaluation

Identity risk evaluation translates authentication attributes and behavioral indicators into a numerical score that represents the likelihood of abnormal session activity. The model integrates authentication factors and behavioral deviations through a combined evaluation process.

The risk calculation follows the equation introduced in the methodology:

$R_i = \alpha A_i + \beta B_i$

In this expression, R_i represents the risk score assigned to identity session i. The variable A_I represents authentication-related irregularities such as unfamiliar devices or unusual login locations. The variable Bi represents behavioral deviations detected during session activity. The parameters α and β represent weighting coefficients that determine the relative influence of authentication and behavioral factors. Risk scores for enterprise sessions ranged between 0 and 1. Sessions with consistent authentication attributes and stable behavioral patterns produced low risk scores. Sessions containing unusual login characteristics or behavioral anomalies produced higher scores.

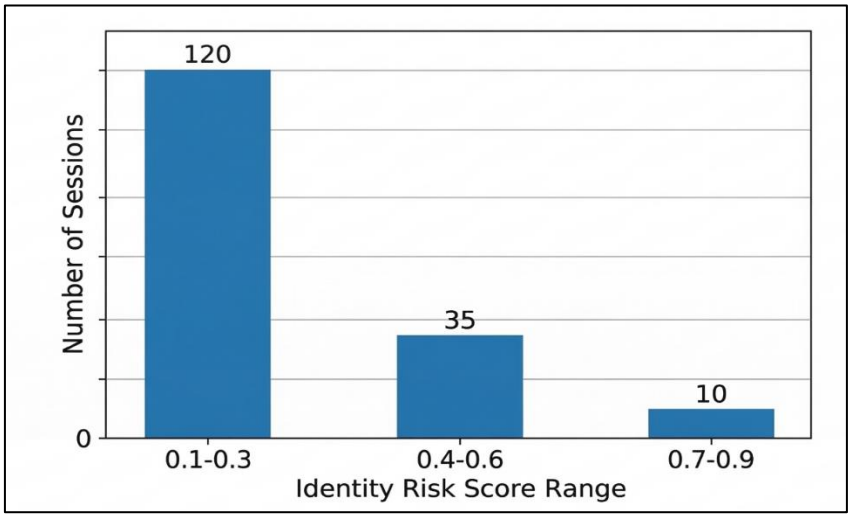

Figure 4: Identity Risk Score Distribution Across Enterprise Sessions

Figure 4 illustrates the distribution of calculated risk scores across enterprise sessions. The majority of sessions fall within the low-risk range between 0.1 and 0.3. These sessions correspond to normal user activity that matches established behavioral patterns. A smaller group of sessions appears within the moderate risk range between 0.4 and 0.6. These sessions contain minor irregularities such as temporary device changes or unexpected login times. The monitoring system marks these sessions for additional verification. High-risk sessions above 0.7 correspond to significant deviations from normal behavior. Examples include repeated authentication failures followed by successful login attempts from new locations or irregular resource access patterns. These sessions triggered policy-based restrictions within the system.

Risk evaluation also supports identity trust interpretation. A simple trust measure is defined as:

$$Ti = 1 - Ri$$

In this equation, Ti represents the trust value associated with identity session i Lower risk scores correspond to higher trust levels. This relationship provides a convenient method for interpreting risk evaluation results during access decision processes.

C. Access Decision Effectiveness

The policy-based access control component interprets risk scores and determines access permissions for enterprise resources. Security policies define acceptable risk thresholds associated with different categories of enterprise applications. Three access conditions appear in the evaluation. Sessions with low-risk values receive normal access privileges. Sessions with moderate risk values require additional identity verification procedures such as multi-factor authentication. Sessions with high-risk values result in restricted access or session termination. The evaluation demonstrates that the proposed model responds dynamically to changes in identity behavior. Risk values may increase during an active session when behavioral anomalies appear. The policy engine reacts immediately and adjusts access permissions accordingly. This dynamic access control mechanism differs from traditional RBAC systems. RBAC frameworks assign permissions based on predefined user roles. Access privileges remain fixed throughout the session after successful authentication. Such static authorization structures cannot respond to changes in identity behavior during system interaction. The identity-centric model evaluates identity conditions continuously. This capability allows the system to restrict access when suspicious activity appears even after successful login. The results indicate that adaptive policy enforcement reduces the risk of unauthorized activity caused by compromised credentials.

D. Security Performance Discussion

A comparative analysis evaluated the performance of the proposed identity-centric model against conventional RBAC systems. The comparison examined anomaly detection capability, response time to suspicious activity, and access decision accuracy.

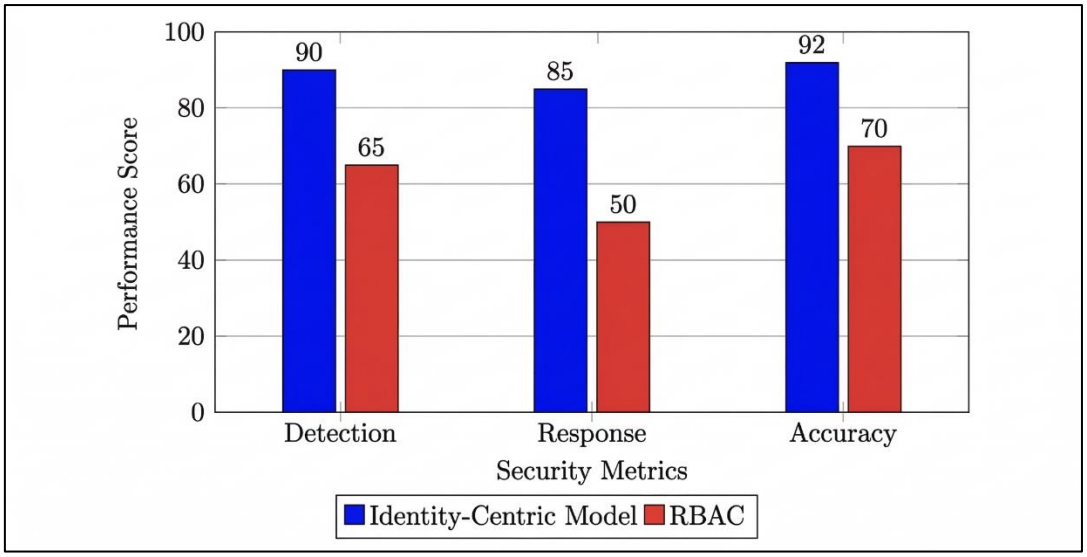

Figure 5: Comparative Security Performance of the Proposed Model vs Traditional RBAC

Figure 5 presents the performance comparison between the two security models. The identity-centric approach detects abnormal activity patterns more effectively because the system evaluates both authentication attributes and behavioral indicators. RBAC systems depend primarily on user roles and initial authentication events. Response time also differs between the models. Continuous monitoring allows the identity-centric system to react immediately when risk scores exceed defined thresholds. RBAC systems require administrative intervention or external monitoring tools to detect suspicious activity. Table 2 summarizes the observed performance differences.

Table 2: Security Performance Comparison Between Identity-Centric Model and RBAC

Security Metric	Identity-Centric Model	Traditional RBAC
Anomaly Detection Capability	High	Moderate
Response Time to Suspicious Activity	Immediate automated response	Delayed manual response
Access Decision Accuracy	Context-aware evaluation	Role-based evaluation
Resistance to Credential Misuse	High	Moderate

The comparison shows that identity-centric monitoring supports more accurate detection of abnormal activity. Behavioral analysis and contextual identity information contribute to improved evaluation of session activity. Risk scoring and policy-based decision mechanisms also allow rapid reaction to suspicious behavior. Identity profiling also plays an important role in the evaluation process. Profiles containing device information, historical login behavior, and access patterns provide contextual information for behavioral analysis. The policy engine uses this information during access decision evaluation. Overall, the results demonstrate that identity-centric security models provide stronger protection for enterprise web systems than static authentication frameworks. Continuous identity evaluation and adaptive access control mechanisms allow the system to react to changing session conditions.

E. Limitations of the Study

Several limitations influence the interpretation of the results presented in this study. The evaluation relies on simulated enterprise session datasets rather than operational enterprise systems. Real enterprise environments contain more complex identity structures, application dependencies, and network configurations. The dataset also represents a limited range of behavioral patterns and authentication scenarios. Larger datasets may reveal additional anomaly characteristics and risk patterns. Integration challenges may also appear in organizations that operate legacy systems lacking support for identity-centric monitoring frameworks. Future research may explore large-scale enterprise deployments, cross-organizational identity relationships, and advanced behavioral analysis techniques that support adaptive identity risk evaluation.

V. CONCLUSION

This study presented an identity-centric security model for enterprise web systems operating in distributed computing environments. The framework integrates identity authentication, identity profiling, behavioral monitoring, risk evaluation, and policy-based access control within a unified security structure. The results show that continuous identity evaluation provides stronger protection than traditional role-based access control systems that depend on static authentication and fixed permission assignments. Behavioral observation identifies irregular activity patterns during active sessions, while risk scoring converts identity conditions into measurable security indicators. The policy engine

interprets these indicators and adjusts access permissions according to predefined security thresholds. The assessment indicates an enhancement of the anomaly detection ability, reaction time to detected anomalies, and accuracy of decisions regarding access. Integrating identity attributes with behavioral factors enables enterprise systems to understand user activities with greater context awareness and operational clarity.

The future research may involve testing the proposed model in a large-scale enterprise environment with varied application environments and identity relationships. Expanded datasets may reveal additional behavioral patterns and security scenarios not captured in the present evaluation. Machine learning methods could support automated behavioral modeling and more precise anomaly detection within enterprise systems. Integration with cloud-native identity platforms and zero-trust security architectures also presents an area for further investigation. Additional studies may analyze cross-organizational identity interactions, federated identity environments, and scalable identity governance mechanisms suitable for large enterprise infrastructures.

REFERENCES

1. Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005
2. Hasan, E. (2025). Secure and scalable data management for digital transformation in finance and IT systems. *Zenodo*. https://doi.org/10.5281/zenodo.17202282
3. Joarder, M. M. I. (2025). Disaster recovery and high-availability frameworks for hybrid cloud environments. *Zenodo*. https://doi.org/10.5281/zenodo.17100446
4. Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT-based electric vehicle ecosystems. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184
5. Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 127–140. https://doi.org/10.30574/wjaets.2025.17.2.1475
6. Zaman, S. U. (2025). Vulnerability management and automated incident response in corporate networks. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(5), 2275–2286. https://doi.org/10.5281/zenodo.17536305
7. Punia, A., Gulia, P., Gill, N. S., et al. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing, 13*, 146. https://doi.org/10.1186/s13677-024-00697-7
8. Zaman, S. U. (2025). Enhancing security in cloud-based IAM systems using real-time anomaly detection. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883
9. Rahman, T. (2026). Financial risk intelligence: Real-time fraud detection and threat monitoring. *Zenodo*. https://doi.org/10.5281/zenodo.18176490
10. Zwattendorfer, B., Tauber, A., & others. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering, 66*, 421–440. https://doi.org/10.1007/s12599-023-00830-x
11. Zaman, S. U., Afrin, S., Zaidi, S. K. A., & Islam, K. S. A. (2026). Resilient edge computing framework for autonomous, secure, and energy-aware systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 105–121. https://doi.org/10.30574/wjaets.2026.18.1.1577
12. Fahim, M. A. I., Farooq, H., & Sharan, S. M. M. I. (2026). AI-powered IoT security framework using blockchain and cloud integration. *Global Journal of Engineering and Technology Advances, 26*(1), 168–185. https://doi.org/10.30574/gjeta.2026.26.1.0003
13. Zaidi, S. K. A., Islam, K. S. A., Zaman, S. U., & Afrin, S. (2026). Blockchain-secured communication for industrial IoT and aviation control systems. *International Journal of Scientific Research and Engineering Development (IJSRED), 9*(1), 234–250. https://doi.org/10.5281/zenodo.18278261
14. Nahar, S., Rahman, M., Alam, M. S., & Al Sany, S. M. A. (2026). Intelligent data governance and ethical AI framework for enterprise information systems. *Zenodo*. https://doi.org/10.5281/zenodo.18839122
15. Enam, M. M. R., Joarder, M. M. I., Taimun, M. T. Y., & Sharan, S. M. I. (2025). Framework for smart SCADA systems: Integrating cloud computing, IIoT, and cybersecurity for enhanced industrial automation. *Saudi Journal of Engineering and Technology, 10*(4), 152–158.
16. Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering, 2*(11), 220–242. https://doi.org/10.70849/IJSCI02112025025
17. Liu, X., et al. (2025). An ⟨entity, organization⟩ integrated access control model. *Computers & Security*. https://doi.org/10.1016/j.cose.2025.104799
18. Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458
19. Afrin, S. (2025). Cloud-integrated network

monitoring dashboards using IoT and edge analytics. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(5), 2298–2307. https://doi.org/10.5281/zenodo.17536343

20. Fahim, M. A. I., Sharan, S. M. M. I., & Farooq, H. (2025). AI-enabled cloud-IoT platform for predictive infrastructure automation. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 431–446. https://doi.org/10.30574/wjaets.2025.17.3.1574
21. Rahman, M. (2025). Design and implementation of a data-driven financial risk management system for
22. U.S. SMEs using federated learning and privacy-preserving AI techniques. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(6), 1041–1052. https://doi.org/10.5281/zenodo.17769869
23. Islam, R. (2025). AI and big data for predictive analytics in pharmaceutical quality assurance. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319
24. Akhter, T. (2025, October 6). Algorithmic internal controls for SMEs using MIS event logs. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978941.15848264.v1
25. Rahman, M., Haque, S., & Al Sany, S. M. A. (2025). Federated learning for privacy-preserving apparel supply chain analytics. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386
26. Rahman, F., Nahar, S., & Mim, M. A. (2026). Cloud-native enterprise resource management for multi-sector operations. *Global Journal of Engineering and Technology Advances, 26*(1), 126–141. https://doi.org/10.30574/gjeta.2026.26.1.0012
27. Sharan, S. M. M. I., Fahim, M. A. I., & Farooq, H. (2026). Cloud native fintech analytics platform for IoT enabled retail networks. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 89–104. https://doi.org/10.30574/wjaets.2026.18.1.1582
28. Dukkipati, S. S. N. C. (2026, February 9). Design and implementation of scalable AI-driven conversational systems for enterprise-level feedback intelligence and decision support. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6263818
29. Tabassum, M., Rokibuzzaman, M., Islam, M. I., & Bristy, I. J. (2025). Data-driven financial analytics through MIS platforms in emerging economies. *Saudi Journal of Engineering and Technology, 10*(9), 440–446. https://doi.org/10.36348/sjet.2025.v10i09.007
30. Tabassum, M., Islam, M. I., Bristy, I. J., & Rokibuzzaman, M. (2025). Blockchain and ERP-integrated MIS for transparent apparel & textile supply chains. *Saudi Journal of Engineering and Technology, 10*(9), 447–456. https://doi.org/10.36348/sjet.2025.v10i09.008
31. Hasan, E. (2025). Big data-driven business process optimization: Enhancing decision-making through predictive analytics. *TechRxiv*. https://doi.org/10.36227/techrxiv.175987736.61988942/v1
32. Hasan, E. (2025). SQL-driven data quality optimization in multi-source enterprise dashboards. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(6), 2150–2160. https://doi.org/10.5281/zenodo.17926758
33. Hasan, E. (2025). Machine learning-based KPI forecasting for finance and operations teams. *International Journal of Scientific Research and Engineering Development (IJSRED), 8*(6), 2139–2149. https://doi.org/10.5281/zenodo.17926746
34. Nahar, S., Rahman, M., Alam, M. S., & Al Sany, S. M. A. (2026). Intelligent data governance and ethical AI framework for enterprise information systems. *Zenodo*. https://doi.org/10.5281/zenodo.18839122
35. Islam, R. (2026). AI-integrated management information systems for manufacturing and supply chain risk mitigation. *Zenodo*. https://doi.org/10.5281/zenodo.18349501
36. Afrin, S., Zaman, S. U., Islam, K. S. A., & Zaidi, S. K. A. (2026). Distributed edge intelligence for energy and transportation systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 280–297. https://doi.org/10.30574/wjaets.2026.18.1.0049

