An Intelligent Role-Based Access Control Model Enhanced with Risk-Based Multi-Factor Authentication

[1]Maduabuchukwu Christopher, *[1]Anazia Eluemunor Kizito and [2]Nwokolo Geofrey Augustine

[1]Department of Information Systems and Technology Southern Delta University, Ozoro

[2]Department of Data Science Southern Delta University, Ozoro

***Correspondence Author**

DOI: https://doi.org/10.51584/IJRIAS.2026.110400057

Received: 11 April 2026; Accepted: 16 April 2026; Published: 04 May 2026

ABSTRACT

This study presents an Intelligent Role-Based Access Control model enhanced with Risk-Based Multi-Factor Authentication (R-MFA) to overcome the limitations of traditional Role-Based Access Control (RBAC) and standard role-based access control with Multi-Factor Authentication (MFA) approaches. The model combines structured authorization with adaptive, context-aware authentication to achieve a better balance between security and system performance. Its effectiveness was assessed by comparing it with traditional role-based access control and role-based access control integrated with multi-factor authentication using key performance metrics such as authentication time, access success rate, false acceptance rate (FAR), system throughput, and security strength index. The findings reveal that traditional role-based access control offers the fastest authentication time (1.2 seconds) and highest throughput (120 requests per second), but suffers from weaker security, with a 6.5% FAR and a security strength index of 68.0%. The introduction of standard multi-factor authentication improves security, increasing the success rate to 96.2% and reducing FAR to 3.1%, although it leads to higher authentication time (3.8 seconds) and lower throughput (95 requests per second). In contrast, the Intelligent role-based access control model enhanced with risk-based multi-factor authentication achieves a more balanced outcome, delivering a 97.8% success rate, a low FAR of 1.2%, moderate authentication time of 2.4 seconds, throughput of 110 requests per second, and the highest security strength index of 94.2%. Overall, the results highlight the model's ability to enhance security without significantly compromising system efficiency.

Keywords: Access Control, Role-Based Access Control, Multi-Factor Authentication, Intelligent Role-Based Access Control, Risk-Based Multi-Factor Authentication.

INTRODUCTION

The rapid growth of digital technologies, cloud computing, and distributed systems has made securing modern information systems far more challenging than ever before. Organizations now operate in highly interconnected environments where threats such as unauthorized access, credential theft, insider misuse, and advanced persistent attacks are increasingly common. These evolving risks make it essential to adopt strong and reliable access control mechanisms that can safeguard sensitive data while preserving confidentiality, integrity, and availability (Pranggono & Arabo, 2020).

One of the most widely used approaches to managing access is role-based access control. Its appeal lies in its simplicity and structure, as permissions are assigned to roles rather than individual users. This not only reduces administrative burden but also supports the principle of least privilege by ensuring users have only the access necessary to perform their duties (Kumar, 2025; Anazia et al., 2025). However, traditional role-based access control systems are largely static and struggle to adapt to dynamic environments such as cloud platforms and Internet of Things (IoT) ecosystems, where access decisions often need to reflect changing contexts (Cobrado et al., 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

To strengthen user authentication, multi-factor authentication has become a widely adopted security measure. By requiring multiple forms of verification, such as passwords, tokens, or biometrics, multi-factor authentication significantly reduces the likelihood of unauthorized access (Suleski et al., 2023). Studies have consistently shown that multi-factor authentication offers stronger protection than single-factor authentication (Akpan et al., 2026). However, while multi-factor authentication improves identity verification, it does not account for contextual risk or influence authorization decisions once access is requested.

In response to these limitations, more adaptive approaches such as risk-based access control and risk-based authentication have been developed. These models assess contextual factors, including user behavior, location, and device trust level, before granting access. This allows systems to respond more intelligently to potential threats and adjust security requirements in real time (Oluoha et al., 2022; Anazia et al., 2026). Similarly, the Zero Trust Architecture model reinforces the idea that no user or system should be automatically trusted, emphasizing continuous verification regardless of network location (Mao, 2025).

Despite these advancements, many existing solutions treat role-based access control, multi-factor authentication, and risk-based models as separate layers rather than parts of a unified system. This fragmented approach can reduce their overall effectiveness in handling complex and evolving security challenges. To address this gap, this study proposes an Intelligent role-based access control model enhanced with risk-based multi-factor authentication. The model integrates role-based authorization, adaptive authentication, and real-time risk evaluation into a cohesive framework, offering a more responsive and robust approach to securing modern information systems.

REVIEW OF RELATED LITERATURE

Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) has long been a practical and widely adopted approach for managing user permissions in enterprise systems. Its strength lies in its simplicity: instead of assigning permissions to individual users, organizations assign them to roles that reflect job responsibilities. This makes access management more organized, reduces administrative workload, and supports consistent policy enforcement (Atlam, 2020 et al.; Eti et al., 2025).

In the work of Anazia et al. (2025), they opined computing environments become more dynamic, the limitations of traditional role-based access control have become more apparent. Because roles are typically predefined and static, they do not easily adapt to changing contexts such as user location, device type, or real-time risk conditions. This rigidity can reduce effectiveness in modern settings like cloud platforms and Internet of Things (IoT) systems, where access decisions often need to be flexible and context-aware (Wiefling et al., 2021). To overcome these challenges, researchers have explored hybrid approaches that extend role-based access control with additional capabilities. For example, integrating role-based access control with Attribute-Based Access Control (ABAC) allows systems to consider attributes such as user behavior, environmental conditions, and resource sensitivity when making access decisions (Abdulrahman & Chen, 2021). More recently, intelligent and AI-driven models have emerged, enabling role-based access control systems to move beyond static rules toward more adaptive and predictive decision-making processes (Zisad & Hasan, 2026).

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) has become a fundamental component of modern cybersecurity strategies because it strengthens the process of verifying user identity. By requiring multiple forms of authentication, such as passwords, tokens, or biometric data, multi-factor authentication adds an extra layer of protection and significantly reduces the chances of unauthorized access, even when credentials are compromised (Behl et al., 2021).

Its importance is particularly evident in sensitive domains such as healthcare, cloud services, and IoT environments. For instance, Alshamrani et al. (2021) highlight how multi-factor authentication helps protect critical patient data in healthcare systems. In addition, adaptive multi-factor authentication techniques have been

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

introduced to adjust authentication requirements based on contextual risk, balancing security with user convenience (Talasila, 2025).

Despite its strengths, multi-factor authentication focuses primarily on verifying identity rather than controlling what an authenticated user is allowed to do. As a result, it does not address authorization in a comprehensive way, which limits its effectiveness when used in isolation.

Risk-Based Access Control and Authentication

According to Anazia et al. (2025), it was noted that risk-based access control represents a more flexible and intelligent approach to security by incorporating context into decision-making. Instead of relying solely on predefined rules, these models evaluate factors such as user location, device trustworthiness, access history, and behavioral patterns to determine the level of risk associated with each access request (Zhang et al., 2021). This dynamic assessment allows systems to respond more effectively to potential threats. For example, risk-based authentication can increase security requirements when suspicious activity is detected, thereby reducing the likelihood of breaches (Li, 2020). The integration of machine learning and artificial intelligence has further strengthened these models by improving their ability to detect patterns, predict risks, and make accurate decisions in real time (Sharma & Gupta, 2023).

Zero Trust Architecture builds on this idea by removing the concept of implicit trust altogether. Under this model, every access request is continuously verified, regardless of where it originates, ensuring a consistently high level of security across the system (Ahmed, 2020).

Integration of Role-Based Access Control, Multi-Factor Authentication and Risk-Based Model

Bringing together role-based access control, multi-factor authentication and risk-based approaches offers a more comprehensive solution to modern security challenges. Each model contributes a unique strength: role-based access control provides structured authorization, multi-factor authentication ensures strong identity verification, and risk-based mechanisms introduce adaptability and context awareness. When combined, they create a more resilient and effective access control framework (Zerkouk et al., 2020; Anazia, 2026).

Research has shown that integrating multi-factor authentication with role-based access control improves security outcomes compared to using either approach alone (Verma & Hossain 2021). Similarly, risk-aware role-based access control models introduce dynamic decision-making into traditionally static systems, allowing them to respond to evolving threats (Khanet al., 2022).

Nevertheless, achieving full integration remains challenging. Many existing solutions struggle with increased system complexity, performance overhead, and the difficulty of processing risk factors in real time. In addition, authentication and authorization are often still treated as separate processes rather than components of a unified system (Gasser et al., 2021).

Current research is therefore moving toward intelligent, AI-driven frameworks that can address these challenges by delivering scalable, adaptive, and context-aware access control solutions (Okpor et al, 2024).

Overall, the review shows that while role-based access control, multi-factor authentication, and risk-based models each offer valuable benefits, they also have clear limitations when used independently. There remains a noticeable gap in fully integrated systems that unify these approaches into a single, intelligent framework. This study seeks to address that gap by proposing a model that enhances security while maintaining flexibility and scalability in modern computing environments

METHODOLOGY

Research Design

The research design follows a structured approach to develop and validate an intelligent access control model. It begins with an analysis of existing approaches such as role-based access control, multi-factor authentication,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

and risk-based models, revealing key limitations including limited adaptability, weak integration, and poor context awareness. From this, the study establishes core system requirements, including role and permission management, multi-factor authentication, contextual risk evaluation based on factors like location and behavior, and real-time decision-making capability.

Based on these requirements, a hybrid model is designed to integrate role-based access control for structured authorization, multi-factor authentication for strong identity verification, and a risk-based engine for adaptive access control. These components are unified through an intelligent decision layer that evaluates contextual risk and supports dynamic, informed access decisions.

The implementation phase translates this conceptual design into a functional system using a modular architecture that supports flexibility and scalability. The system can be developed using common backend technologies such as Python, Java, or Node.js, with databases like MySQL or PostgreSQL for efficient data management. Authentication is handled through various mechanisms, including one-time passwords, biometric simulations, and token-based methods, while the risk evaluation component is implemented using either rule-based logic or machine learning techniques to analyze and respond to different risk conditions.

Finally, the system is tested under different scenarios, ranging from low-risk to high-risk conditions, to evaluate its ability to adapt to varying contexts while maintaining strong security and usability.

Performance Evaluation

The performance of the model will be evaluated using a combination of quantitative metrics and comparative analysis to ensure a comprehensive and reliable assessment. Key evaluation parameters include authentication time, access success rate, false acceptance rate (FAR), system throughput, and security strength index. These metrics are deliberately selected to capture both the security robustness and operational efficiency of the system, providing a well-rounded basis for evaluation. To validate its effectiveness, the intelligent multi-factor authentication model will be benchmarked against two established approaches: the traditional role-based access control model and role-based access control model integrated with standard multi-factor authentication. This comparative framework enables a clear assessment of performance improvements and trade-offs, particularly in terms of security enhancement and system efficiency.

Mathematical Representation of the Model

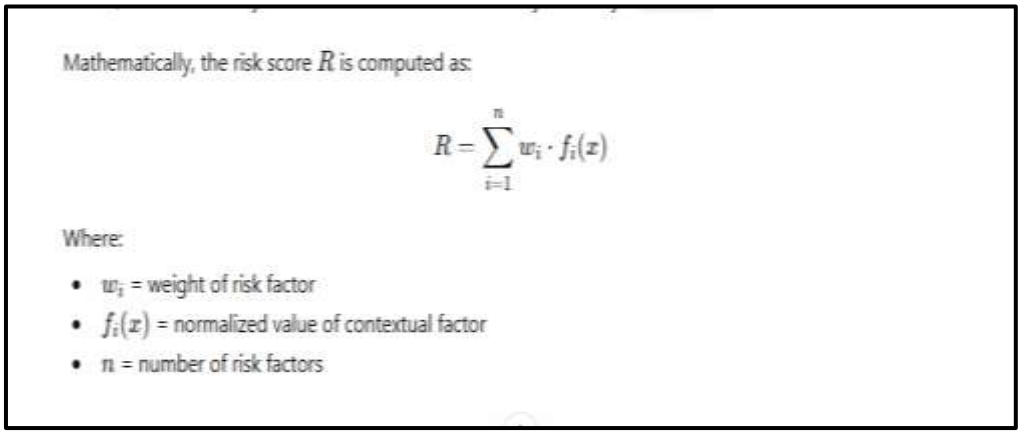

Fig 1: Mathematical Representation of the Model

The diagram can be expressed mathematically as a decision function where access is determined by user identity, contextual risk, and policy rules. Let $A=f(U, C, P)$ where U represents user credentials, C the contextual risk factors, and P the policy set. Authentication is modeled as a Boolean function $Auth(U)$, which must be true for further evaluation. If the risk function $R=g(C)$ indicates high risk, an additional condition $MFA(U)$ is required. The final access decision is therefore given by $A=Auth(U) \wedge (R=Low \vee MFA(U)) \wedge Policy(U,P)$, where access is granted only if all conditions are satisfied; otherwise, it is denied.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

System Architectural Design

The system adopts a layered architecture to ensure modularity, flexibility, and scalability in access control management. Each module handles a specific function, including user interaction, authentication, risk assessment, authorization, and data management, allowing the system to operate in a structured and coordinated manner. This design promotes clear separation of responsibilities, making the system easier to maintain and extend. It also supports real-time processing of access requests, enabling quick and adaptive responses to changing security conditions while maintaining overall efficiency.

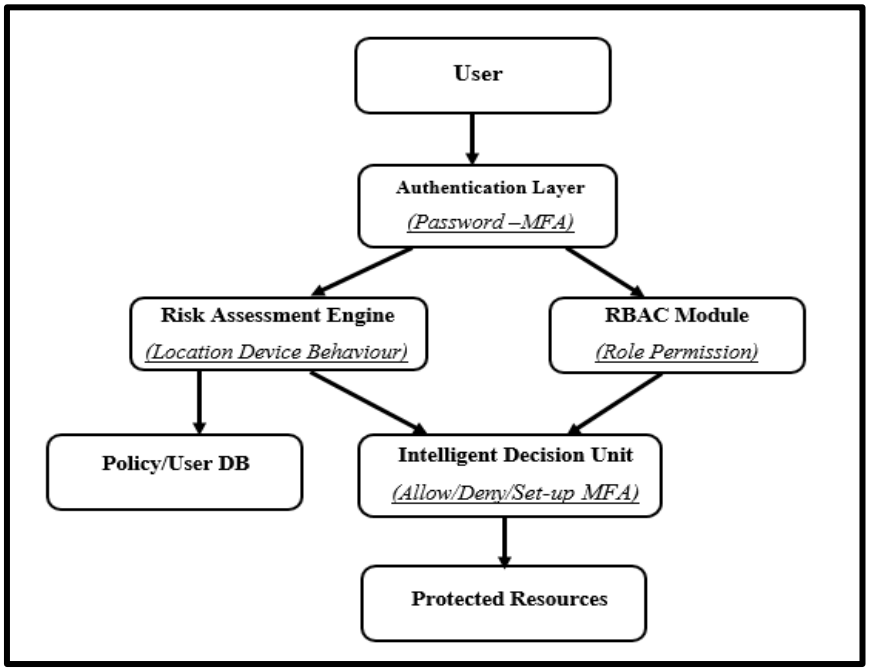

Fig 2: The System's Architecture

System's Components

i. **User Module:** The user represents any individual or entity seeking access to the system's protected resources. The entire process begins at this module where users submits credentials through an interface such as a login portal or application endpoint. The quality and legitimacy of these inputs set the tone for the entire security process, determining whether the request advances to deeper verification stages.

ii. **Authentication Module:** The authentication module, strengthened with multi-factor authentication, is responsible for confirming the user's identity using multiple forms of evidence. This may include something the user knows, like a password, something the user has, such as a token or one-time password, and in some cases something the user is, such as biometric data. By combining these factors, the system significantly reduces the risk of unauthorized access and establishes a strong initial line of defense.

iii. **Risk Assessment Module:** The risk assessment module adds an adaptive dimension to the system by evaluating the context of each access request. It considers factors such as the user's location, device reliability, and behavioral patterns, including login timing and frequency. From this information, it generates a risk score that reflects how trustworthy the request appears. This allows the system to move beyond fixed rules and respond intelligently to changing conditions in real time.

iv. **The Role-Based Access Control Module:** The role-based access control module serves as the foundation for authorization by determining what an authenticated user is allowed to access. It assigns users to roles and links each role to specific permissions, ensuring that access rights align with defined responsibilities. This structured approach simplifies management while reinforcing the principle of least privilege, limiting unnecessary exposure to sensitive resources.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

v. **The Intelligent Decision Module:** At the centre of the system is the intelligent decision unit, which brings together inputs from authentication, risk evaluation, and authorization. Rather than treating these elements separately, it evaluates them collectively to decide whether to grant access, deny it, or request additional verification. This ensures that every decision reflects a complete view of identity, context, and permission.

vi. **Protected Resources Module:** This protected resources represent the assets the system is designed to safeguard, including databases, applications, files, and network services. Access to these resources is only granted after all security checks have been successfully completed, ensuring that critical information remains secure, consistent, and available only to authorized users.

vii. **Policy and User Database Module**: Supporting these processes is the Policy and User Database, which acts as the central repository of system information. It stores user identities, role assignments, access policies, authentication logs, and historical behavioral data. Both the role-based access control engine and the risk assessment engine continuously interact with this database to retrieve relevant information and update records after each access attempt. This persistent data storage enables learning and improvement in risk evaluation over time.

Workflow Diagram

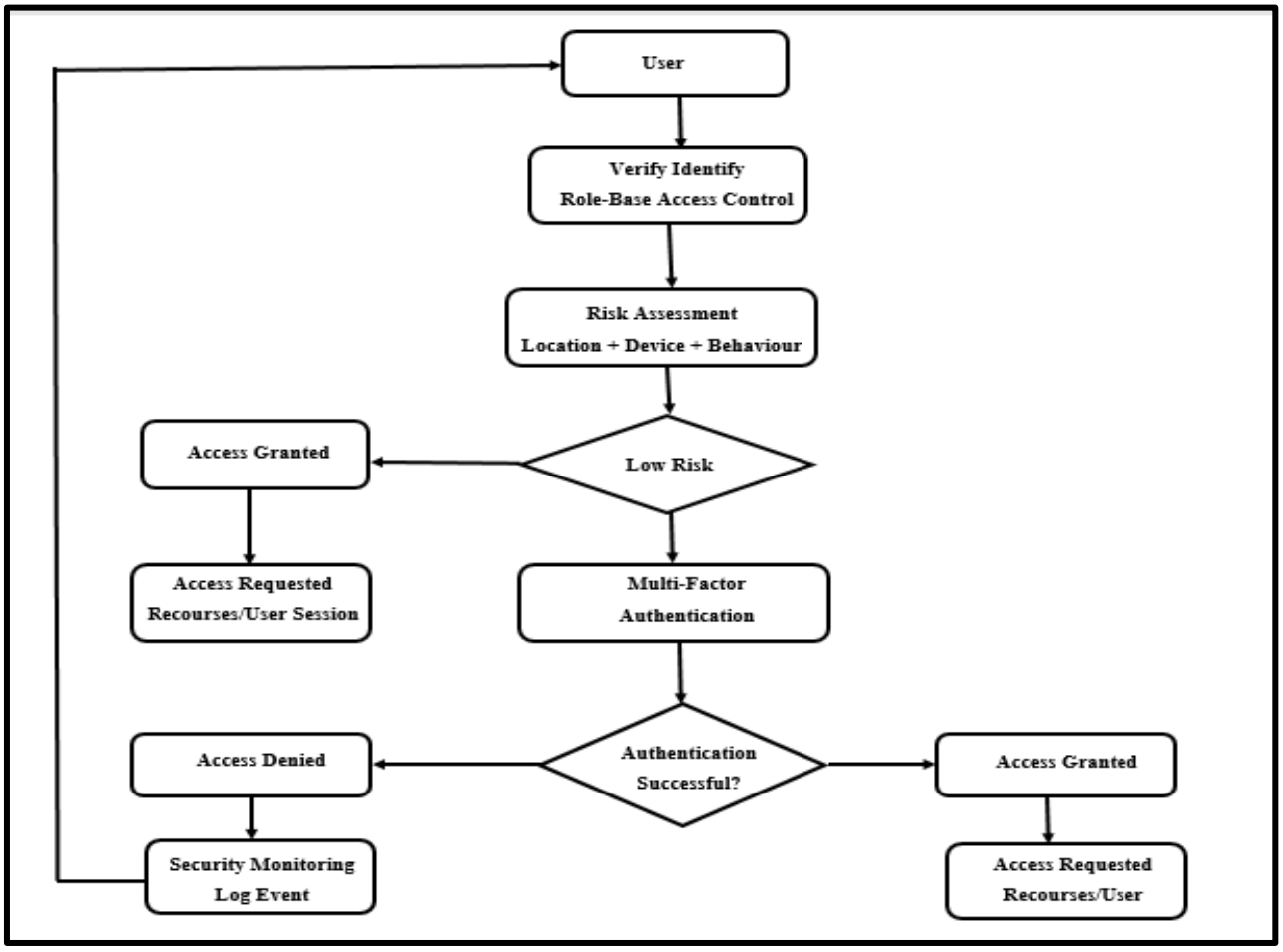

Fig 3: The Workflow of the Model

The workflow begins when a user submits login credentials. The system verifies identity and checks permissions using role-based access control. Instead of granting access immediately, the request is evaluated through a risk assessment that considers factors like location, device and user behavior to generate a risk score. Low-risk requests are granted directly, while medium or high-risk cases trigger multi-factor authentication for additional verification. Access is granted only if this step is successfully completed; otherwise, the request is denied and logged.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

Overall, the approach combines role-based control, contextual risk analysis and multi-factor authentication to deliver a secure and user-friendly access system.

RESULTS AND DISCUSSION

Table 1: The performance metrics of Traditional RBAC, RBAC + Standard MFA and Intelligent RBAC with R-MFA

S/N	Metric	Traditional RBAC	RBAC + Standard MFA	Intelligent RBAC with R-MFA
1	Authentication Time (sec)	1.2	3.8	2.4
2	Access Success Rate (%)	92.5	96.2	97.8
3	False Acceptance Rate (FAR) (%)	6.5	3.1	1.2
4	System Throughput (req/sec)	120	95	110
5	Security Strength Index (%)	68.0	82.5	94.2

The experimental evaluation compared three access control approaches, namely the traditional role-based access control, role-based access control integrated with standard multi-factor authentication and the Intelligent role-based access control model enhanced with risk-based multi-factor authentication. The comparison was conducted using five key performance metrics: authentication time, access success rate, false acceptance rate (FAR), system throughput and security strength index.

The role-based access control model recorded an authentication time of 1.2 seconds, indicating a relatively fast authentication process due to its reliance on single-factor or static credential verification. However, this speed comes at the expense of security robustness, as reflected in its lower access success rate of 92.5% and a relatively high false acceptance rate of 6.5%. The system throughput was highest at 120 requests per second, demonstrating efficiency in handling user requests. Despite this performance advantage, the security strength index remained comparatively low at 68.0%, highlighting the inherent limitations of traditional RBAC in addressing modern, context-aware security threats.

The integration of standard multi-factor authentication into role-based access control significantly improved security-related metrics. The access success rate increased to 96.2%, while the false acceptance rate decreased to 3.1%, indicating enhanced authentication reliability. Additionally, the security strength index improved markedly to 82.5%. However, these gains introduced performance trade-offs. The authentication time increased substantially to 3.8 seconds due to the additional verification layers, and system throughput declined to 95 requests per second. This reflects the common challenge in security systems where stronger authentication mechanisms often lead to reduced system efficiency and increased user friction.

In contrast, the Intelligent role-based access control model with risk-based multi-factor authentication demonstrated a more balanced performance across all metrics. The authentication time was reduced to 2.4 seconds compared to standard multi-factor authentication, indicating improved efficiency through adaptive authentication processes that apply stricter controls only when necessary. The model achieved the highest access success rate of 97.8% and the lowest false acceptance rate of 1.2%, confirming its effectiveness in accurately distinguishing legitimate users from unauthorized attempts. Furthermore, the system maintained a high throughput of 110 requests per second, outperforming the standard multi-factor authentication -enhanced role-based access control. Most notably, the security strength index reached 94.2%, representing a substantial improvement over both baseline and conventional multi-factor authentication models.

Overall, the results demonstrate that while traditional role-based access control offers superior speed and throughput, it lacks sufficient security strength for contemporary systems. The addition of standard multi-factor

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

authentication improves security but introduces significant performance overhead. The Intelligent role-based access control with risk-based multi-factor authentication effectively addresses this trade-off by leveraging contextual risk assessment to dynamically adjust authentication requirements, thereby achieving both strong security and acceptable system performance. This balance makes it a more suitable solution for modern secure systems that demand both usability and robust protection.

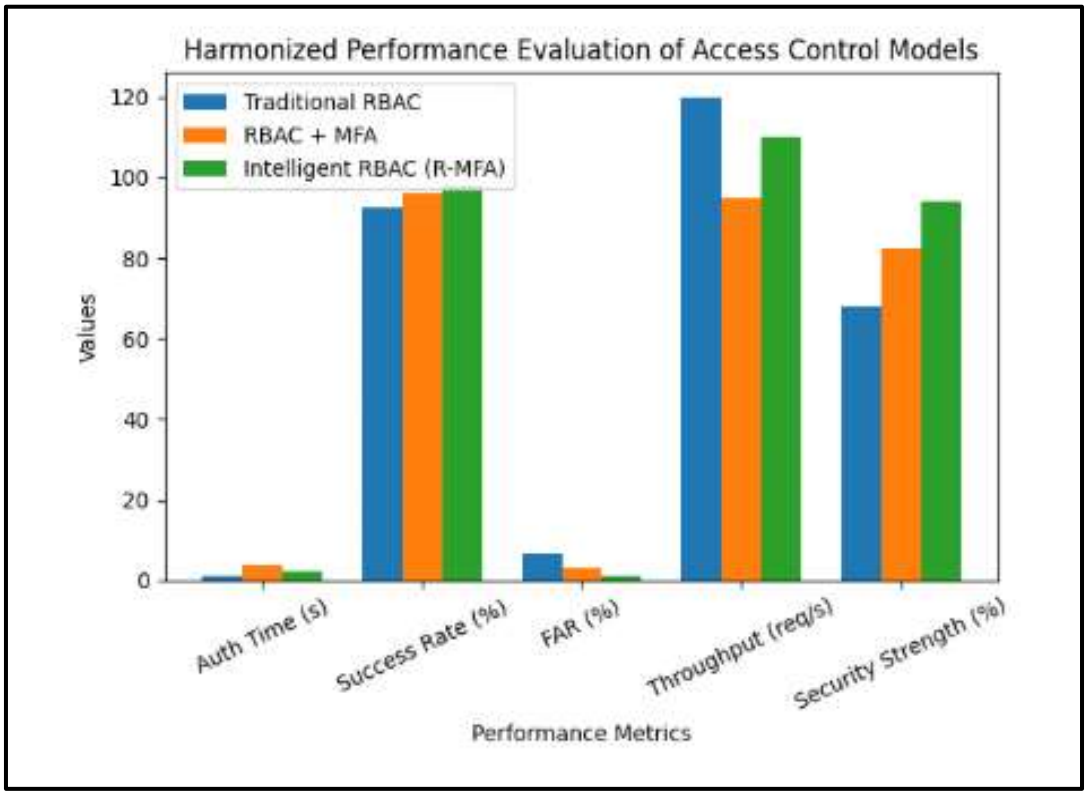

Fig 4**:** A bar chart showing the performance metrics of Traditional RBAC, RBAC + Standard MFA and Intelligent RBAC with R-MFA

Summary

This study evaluated the performance of three access control models, namely traditional role-based access control, role-based access control integrated with standard multi-factor authentication, and an Intelligent role-based access control model enhanced with risk-based multi-factor authentication. The findings show that while the traditional role-based access control model provides faster authentication and higher system throughput, it suffers from weaker security performance, as indicated by a higher false acceptance rate and lower security strength index. The incorporation of standard multi-factor authentication significantly improves security metrics, including access success rate and resistance to unauthorized access, but introduces increased authentication time and reduced throughput. In contrast, the Intelligent role-based access control with risk-based multi-factor authentication achieves a more optimal balance by maintaining strong security performance while reducing the efficiency penalties typically associated with conventional multi-factor authentication. This is evident in its high access success rate, minimal false acceptance rate, improved throughput, and the highest recorded security strength index among the evaluated models.

CONCLUSION

The comparative analysis demonstrates that the limitations of traditional role-based access control and the performance overhead of standard multi-factor authentication can be effectively addressed through the integration of risk-based adaptive authentication mechanisms. The Intelligent role-based access control model enhanced with risk-based multi-factor authentication outperforms the other models by dynamically adjusting authentication requirements based on contextual risk factors. This approach not only strengthens system security but also preserves system usability and efficiency. The results confirm that adaptive, context-aware access

control mechanisms represent a significant advancement over static and uniformly applied authentication models, making them more suitable for modern, security-sensitive environments.

RECOMMENDATIONS

It is recommended that organizations transition from traditional role-based access control systems to more adaptive access control frameworks that incorporate risk-based authentication mechanisms. While standard multi-factor authentication should be adopted as a minimum security requirement, its limitations in terms of performance overhead should be carefully managed. The implementation of Intelligent role-based access control with risk-based multi-factor authentication is strongly encouraged, particularly in environments where both security and system performance are critical. Additionally, future research should explore the integration of machine learning techniques for more accurate risk assessment, as well as real-time behavioral analytics to further enhance authentication decisions. System designers should also focus on optimizing user experience by minimizing unnecessary authentication steps for low-risk access scenarios while maintaining strict controls for high-risk conditions.

Limitations of the Study

Despite its improved performance, the model still presents several limitations. For instance, the evaluation was conducted in a controlled environment, which may not fully capture the complexities and scalability requirements of real-world systems. The effectiveness of the risk assessment also relies on selected contextual factors, such as user behaviour and location, which may be insufficient to detect more sophisticated or evolving threats. In addition, the continuous risk evaluation process introduces computational overhead that could affect overall system efficiency. From a usability standpoint, users in higher-risk scenarios may be required to complete additional authentication steps, potentially reducing convenience. Finally, the study's comparative analysis is limited to RBAC and RBAC with MFA, without incorporating other advanced access control models.

REFERENCE

1. Abdulrahman, M., & Chen, X. (2021). Hybrid access control models integrating RBAC and ABAC for dynamic environments. Journal of Information Security and Applications, 58, 102–115.
2. Ahmed, M., Mahmood, A. N., & Hu, J. (2020). A survey of network anomaly detection. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
3. Akpan, E. J., Okon, B. E., & Udoh, M. S. (2026). Enhancing system security using multi-factor authentication in role-based access control systems. International Journal of Cybersecurity Research, 12(2), 45–60.
4. Alshamrani, A., Myneni, S., Chowdhury, A., & Huang, D. (2021). A survey on advanced authentication techniques for healthcare systems. Healthcare Informatics Research, 27(1), 1–15.
5. Anazia, E. K., Ubrurhe, O., Idama, R. O., & Maduabuchukwu, C. (2025). An optimized encryption model for a robust and efficient information security system. Nigerian Journal of Science and Environment, 23(3).
6. Anazia, E. K., Idama, R. O., Adigwe, W., & Ifeose, J. (2026). FOODCARDQR: A secured student food card management and payment system using QR code authentication. FUDMA Journal of Sciences (FJS), 10(1), 333–339. https://doi.org/10.33003/fjs-2026-0912-4341
7. Anazia, K. E., Maduabuchukwu, C., Francis, O. I., Benafa, C, F., Idama, R., & Eti, F. I. (2025). A novel mobile-based blood donation model for emergency situations. International Journal of Engineering and Computer Science, 14(10). https://doi.org/10.18535/ijecs/v14i10.5288
8. Anazia, K. E. (2026). Smart governance in Nigerian higher education: Integrating artificial intelligence for integrity and effective university leadership. International Journal of Innovative Science and Research Technology, 11(2), 66–74. https://doi.org/10.38124/ijisrt/26feb106
9. Anazia, K. E., Ubrurhe, O., Eti, I. F., Okeke, V. O., & Francis, O. I., (2025). A hybrid algorithm for improving recognition system in human activities. International Journal

of Multidisciplinary Research and Growth Evaluation, 6(3), 584–591. https://doi.org/10.54660/IJMRGE.2025.6.3.584-591

10. Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2020). Integration of cloud computing with internet of things: Challenges and open issues. Future Internet, 12(6), 103. https://doi.org/10.3390/fi12060103
11. Behl, A., Jayawardena, C., & Pereira, V. (2021). Cybersecurity resilience through multi-factor authentication. Computers & Security, 102, 102152. https://doi.org/10.1016/j.cose.2020.102152
12. Cobrado, L., Ferreira, J., & Antunes, M. (2024). Limitations of traditional RBAC in cloud and IoT environments. Journal of Cloud Computing, 13(1), 1–14.
13. Eti, I. F., Anazia, K. E., Okeke, V. O., Benafa, F. C., & Orugba, K. (2025). A secured blockchain database management model for medical based organization. International Journal of Advances in Engineering and Management (IJAEM), 7(5), 312–323. https://doi.org/10.35629/5252-0705312323
14. Gasser, O., Stransky, C., & Holz, T. (2021). Security implications of adaptive authentication. IEEE Security & Privacy, 19(2), 54–61. https://doi.org/10.1109/MSEC.2021.3050064
15. Khan, M. A., Salah, K., & Jayaraman, R. (2022). Blockchain-based access control. IEEE Access, 10, 12345–12360. https://doi.org/10.1109/ACCESS.2022.3145678
16. Kumar, R. (2025). Role-based access control: Principles, challenges, and future directions. International Journal of Information Security, 24(3), 210–225.
17. Li, X., Jiang, Q., Chen, Y., Luo, X., & Wen, Q. (2020). Efficient dynamic access control for cloud computing. Future Generation Computer Systems, 95, 652–666. https://doi.org/10.1016/j.future.2018.12.021
18. Mao, Y. (2025). Zero trust architecture: Principles and implementation in modern networks. IEEE Security & Privacy, 23(2), 34–42.
19. Okpor, M. D., Anazia, K. E, & Ukpenusiowho, D. (2024**).** A novel hybrid database security management technique. International Journal of Science and Research Archive, 11(2), 1555–1565. https://doi.org/10.30574/ijsra.2024.11.2.0652
20. Oluoha, U. C., Eze, P. C., & Nwankwo, C. (2022). Risk-based access control models for adaptive security systems. African Journal of Computing and ICT, 15(4), 78–90.
21. Pranggono, B., & Arabo, A. (2020). Cyber security challenges and solutions in cloud computing environments. Future Internet, 12(3), 45–60.
22. Sharma, V., & Gupta, R. (2023). Machine learning approaches for risk-based authentication and access control. Journal of Cybersecurity Technology, 7(2), 89–105.
23. Suleski, J., Novak, M., & Petrovic, S. (2023). Multi-factor authentication: A comprehensive review of methods and applications. Computers & Security, 124, 102–118.
24. Talasila, M. (2025). Adaptive multi-factor authentication using contextual risk analysis. Journal of Information Security, 16(1), 55–70.
25. Verma, R., & Hossain, M. S. (2021). Risk-aware access control model for cloud computing. Journal of Network and Computer Applications, 178, 102981. https://doi.org/10.1016/j.jnca.2021.102981
26. Wiefling, S., Lo Iacono, L., & Dürmuth, M. (2021). More than just good passwords? A study on multi-factor authentication usability. Financial Cryptography and Data Security. https://doi.org/10.1007/978-3-662-64331-0_5
27. Zhang, Y., Liu, J., & Chen, X. (2021). Context-aware access control for distributed systems. IEEE Access, 9, 35369–35381. https://doi.org/10.1109/ACCESS.2021.3062845
28. Zerkouk, M., Lefebvre, G., & Cheriet, M. (2020). Behavioral biometrics for continuous authentication. IEEE Access, 8, 109187–109205. https://doi.org/10.1109/ACCESS.2020.3001853
29. Zisad, M., & Hasan, K. (2026a). Intelligent access control systems using artificial intelligence techniques. Journal of Artificial Intelligence and Security, 9(1), 25–40.