Cybersecurity Risks in Identity and Access Management Using an Adaptive Trust Authenticate Protocol

Ranga Premsai,

Maryland, USA,

Premsairanga809@gmail.com

***Abstract*—Identity and Access Management (IAM) systems are critical for safeguarding organizational infrastructure by ensuring that only authorized users access sensitive information and resources. However, traditional IAM protocols often struggle to detect advanced threats such as identity spoofing, privilege escalation, and unauthorized access through stolen credentials. This paper proposes an adaptive trust authentication protocol that addresses these challenges by integrating deep learning-based anomaly detection, user behavior analytics (UBA), and multi-factor authentication (MFA) into the access control process. The protocol utilizes behavioral biometrics and dynamic access control to continuously monitor user actions in real-time, detecting deviations from typical usage patterns indicative of potential threats. A user trust score is dynamically generated based on real-time behavior analysis and MFA results, while behavior patterns are further evaluated using a deep control convolutional network. By combining the trust score with behavioral analytics, the system initiates secure and context-aware authentication of sensitive financial data. Extensive testing of the proposed protocol demonstrates its effectiveness in mitigating internal and external cybersecurity risks, significantly improving detection accuracy and reducing false positives. The novelty of this approach lies in its seamless integration of advanced behavioral analytics, deep learning, and adaptive authentication strategies, offering a robust, scalable, and resilient solution for modern IAM systems.**

***Index Terms*—Identity and Access Management, Multi-Factor Authentication, Deep Learning, Financial Data Security,deep control convolutional network**

I. INTRODUCTION

The rapid evolution of cyber threats poses a significant challenge to the security and reliability of Identity and Access Management (IAM) systems, which serve as the backbone of organizational infrastructure security. Traditional IAM protocols, while effective at enforcing static access control policies, are increasingly inadequate against sophisticated attack vectors such as identity spoofing, privilege escalation, and unauthorized access via stolen credentials. These limitations are particularly concerning in environments where sensitive data, such as financial information, is at risk. To address these challenges, there is a growing need for IAM systems to adopt adaptive, intelligent, and context-aware security mechanisms [1].

This work introduces an adaptive trust authentication protocol that enhances IAM systems by integrating advanced techniques such as deep learning-based anomaly detection, user behavior analytics (UBA), and multi-factor authentication (MFA). The proposed protocol continuously monitors user actions in real-time, utilizing behavioral biometrics and dynamic access control mechanisms to detect deviations from typical usage patterns that may signal potential threats. A user trust score is dynamically generated by combining real-time behavior monitoring with MFA results, and the behavior patterns are further analyzed using a deep control convolutional network. This fusion of behavioral data and trust metrics allows for secure, context-aware authentication processes, particularly for access to sensitive financial data[2-6].

Extensive testing of the protocol demonstrates significant improvements in detecting and mitigating both internal and external cybersecurity risks, reducing the likelihood of false positives while enhancing overall system security [7,8]. The novel approach of seamlessly integrating deep learning models, behavioral analytics, and dynamic authentication strategies establishes a robust and scalable solution for modern IAM systems. By addressing the limitations of traditional protocols and offering resilience against emerging threats, this adaptive trust authentication protocol represents a significant advancement in the field of IAM and enterprise network security[10-15].

The paper begins with an overview of related work, discussing existing Identity and Access Management (IAM) systems and their limitations in addressing modern cybersecurity challenges. The proposed adaptive trust authentication protocol is then introduced, detailing its key components, including deep learning-based anomaly detection, user behavior analytics (UBA), multi-factor authentication (MFA), and dynamic access control mechanisms. The process of generating trust scores and analyzing behavior patterns using deep convolutional networks is explained, followed by the implementation details and experimental setup used to evaluate the protocol's performance. The results and discussion section highlights the effectiveness of the proposed system in detecting threats, reducing false positives, and improving overall security compared to traditional IAM approaches. Finally, the paper concludes by summarizing the contributions and suggesting potential areas for future research, such as scalability and privacy enhancements.

II. RELATED WORKS

The rapid advancement of cloud computing has introduced a new phase of data management and security problems, especially within multi-cloud settings. In this setting, Identity and Access Management (IAM) has become a crucial emphasis, requiring creative solutions to tackle the challenges of maintaining identities across many platforms. A crucial element of this progression is the incorporation of Artificial Intelligence (AI) into Identity and Access Management (IAM) systems. The use of AI methodologies has shown considerable potential in improving IAM security, operational efficacy, and adherence to regulatory requirements. A comprehensive assessment by [15-16] highlights the shortcomings of conventional IAM systems in multi-cloud environments, which often depend on static, rules-based methodologies that cannot accommodate the evolving dynamics of user behavior and threat landscapes. The authors contend that the incorporation of AI into IAM may enable real-time surveillance and adaptive security protocols, enabling organizations to react swiftly to new risks. They emphasize various machine learning methodologies, including supervised and unsupervised learning algorithms, capable of analyzing extensive datasets to detect abnormal access patterns and provide more precise risk evaluations. The results highlight AI's capacity to shift IAM from a reactive to a proactive security framework, hence improving the overall security stance of organizations using multi-cloud systems. Separate notable research examines the impact of AI in enhancing adherence to regulatory frameworks, specifically concentrating on GDPR and HIPAA mandates. The authors claim that AI-driven IAM systems may automate compliance policy enforcement by continually monitoring access to sensitive data and issuing notifications for any anomalous behavior. They reference case studies in which AI has effectively detected unauthorized access attempts and aided compliance assessments, hence reducing the time and effort needed for human evaluations. This automation improves security and reduces the danger of expensive fines linked to non-compliance. The study demonstrates how AI may function as an essential instrument in enabling organizations to fulfil their legal responsibilities while overseeing complex multi-cloud environments. Moreover, [10-15] examines the interoperability concerns presented by multi-cloud settings and the potential role of AI in mitigating these issues. They observe that diverse cloud providers often use disparate IAM methods, resulting in discrepancies in security rules and heightened administrative burdens. The authors propose a centralised IAM system powered by AI that simplifies difficulties and provides a cohesive method for identity management across various cloud platforms. Their research demonstrates that these frameworks may markedly improve operational efficiency via the automation of user provisioning, access control, and policy enforcement. Implementing a unified IAM approach enables organisations to reduce the likelihood of misconfigurations and security vulnerabilities stemming from fragmented systems. The increasing complexity of cyber threats necessitates a reassessment of IAM techniques. Research by [15] indicates that the conventional dependence on static passwords and single-factor authentication methods exposes organizations to considerable vulnerabilities, such as credential theft and unauthorized access. Their results substantiate the premise that AI-augmented IAM systems may use behavioral biometrics and machine learning techniques to provide adaptive authentication methods. These systems may dynamically modify authentication requirements according to risk levels by analyzing user behaviors and environmental variables. An irregular login attempt from an unknown location may initiate supplementary verification procedures, including multifactor authentication (MFA). This adaptive strategy not only fortifies security but also improves the user experience by reducing friction during lawful access requests. The notion of Zero Trust Architecture (ZTA) has gained prominence as organizations aim to reduce risks in multi-cloud systems. A thorough analysis by [09-15] emphasizes how AI-driven IAM systems conform to ZTA principles via the continual validation of user identities and access privileges. The authors contend that the integration of AI with ZTA yields a more robust security framework, adept at resisting advanced assaults. Their examination of AI algorithms for real-time threat detection demonstrates the efficacy of this integrated method in thwarting unauthorized access and data breaches. The study highlights the need to integrate AI into Identity and Access Management strategies as organizations shift to multi-cloud environments and embrace Zero Trust frameworks. The research indicates an increasing agreement on the transformational capability of AI in improving IAM for multi-cloud environments. The incorporation of AI-driven solutions tackles essential issues such as adaptive security, regulatory compliance, interoperability, and sophisticated threat detection. As organizations adopt multi-cloud strategies, this literature analysis underscores the need for novel IAM methodologies that use AI capabilities to guarantee safe, efficient, and compliant access control across various cloud environments.

III. PROPOSED WORK

Identity and Access Management (IAM) systems are essential for safeguarding organizational infrastructure by ensuring that only authorized users can access sensitive data and resources. Traditional IAM systems, however, are often ineffective at detecting advanced threats, such as identity spoofing, privilege escalation, and unauthorized access through stolen credentials. This paper proposes an adaptive trust authentication protocol that integrates deep learning-based anomaly detection, user behavior analytics (UBA), and multi-factor authentication (MFA) to provide continuous, real-time monitoring and context-aware authentication. This approach enhances detection accuracy, reduces false positives, and provides a more secure and resilient solution for modern IAM systems.

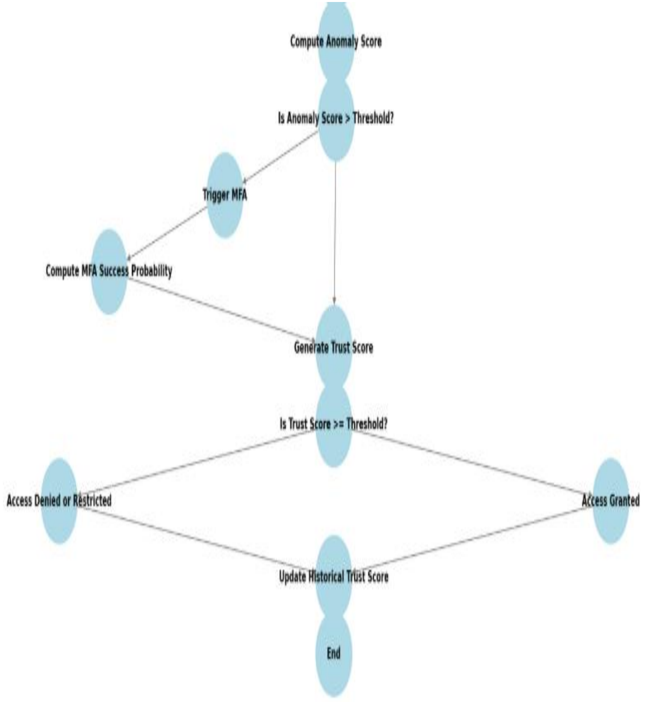

Compute Anomaly Score
Is Anomaly Score > Threshold?
Trigger MFA
Compute MFA Success Probability
Generate Trust Score
Is Trust Score >= Threshold?
Access Denied or Restricted
Access Granted
Update Historical Trust Score
End

Figure 1 Schematic representation of the suggested methodology

Identity and Access Management (IAM) systems are essential for safeguarding organizational infrastructure by ensuring that only authorized users can access sensitive data and resources. Traditional IAM systems, however, are often ineffective at detecting advanced threats, such as identity spoofing, privilege escalation, and unauthorized access through stolen credentials. This paper proposes an adaptive trust authentication protocol that integrates deep learning-based anomaly detection, user behavior analytics (UBA), and multi-factor authentication (MFA) to provide continuous, real-time monitoring and context-aware authentication. This approach enhances detection accuracy, reduces false positives, and provides a more secure and resilient solution for modern IAM systems.

The proposed methodology involves multiple key components that work together to continuously evaluate the trustworthiness of users and their actions. These include:

1. Continuous monitoring and behavioral anomaly detection.
2. Deep learning-based anomaly detection for improved accuracy.
3. User trust scoring, incorporating both behavioral analysis and MFA results.
4. Dynamic access control and context-aware authentication.

A. *Financial Transaction Data*

The adaptive trust authentication protocol continuously monitors real-time user behaviors and financial transactions. The key inputs include:

- Transaction Amount: The monetary value of each transaction initiated by the user.
- Transaction Frequency: The number of transactions performed within a given time.
- Transaction Type: The type of financial transaction (e.g., transfers, purchases, bill payments).
- Transaction Location: The geographic location from which the transaction is initiated (e.g., IP address or GPS data).
- Payment Method: The method used to complete the transaction (e.g., credit card, cryptocurrency).
- Account Balance Fluctuations: Large or sudden changes in account balance.

Each of these features helps to build a baseline profile of the user's normal financial activity, which can then be compared to detect anomalies.

B. *Behavioral Analytics with Financial Data*

The system constructs a baseline model of normal user behavior using the financial transaction data. The feature vector for a user's transaction at time t is:

$$X_t = [a\ \text{Amount}\quad {}_t, \text{Frequency}\quad {}_t, \text{Type}\quad {}_t, \text{Location}\quad {}_t, \text{PaymentMethod}\quad {}_t, \text{BalanceChange}\quad {}_t]$$

The anomaly score $S_{\text{anomaly}}(t)$ measures how much the user's current behavior deviates from the baseline:

$$S_{\text{anomaly}}(t) = \frac{|X_t - X_{\text{avg}}|}{X_{\text{std}}} \qquad (1)$$

Where: - X_{avg} is the user's average transaction data, and $-X_{\text{std}}$ is the standard deviation of the user's transactions.

For more advanced detection, a deep learning model is used to capture complex, non-linear relationships in user behavior. Let the model output be denoted as $\grave{y}_t$, the predicted probability that the transaction at time t is legitimate:

$$\grave{y}_t = f(X_t;\theta) \qquad (2)$$

Where $f(X_t;\theta)$ is the deep neural network model that processes the input features X_t at time t.

The deep learning model is trained using the following loss function:

$$\mathcal{L}(\theta) = -\sum_t \left(y_t \log(\grave{y}_t) + (1 - y_t)\log(1 - \grave{y}_t)\right)$$
(3)

Where y_t is the true label (1 for legitimate, 0 for anomalous).

The trust score is a combination of behavioral analysis and multi-factor authentication (MFA). The behavioral trust score $T_{\text{behavior}}\ (t)$ is inversely related to the anomaly score:

$$T_{\text{behavior}}\ (t) = 1 - S_{\text{anomaly}}\ (t)$$

(4)

The MFA trust score $T_{\text{MFA}}(t)$ is based on the success or failure of the MFA process:

$$T_{\text{MFA}}(t) = \begin{cases} 1 & \text{if MFA succeeds} \\ \text{and } 0 & \text{if MFA fails} \end{cases}$$

(5)

The total trust score $T_{\text{total}}\ (t)$ is a weighted combination of these two scores:

$$T_{\text{total}}\ (t) = \alpha T_{\text{behavior}}\ (t) + (1 - \alpha) T_{\text{MFA}}(t)$$

(6)

Where $\alpha \in [0,1]$ is the weight assigned to behavioral data.

Once the trust score is calculated, the system makes an access decision based on the required trust threshold R_{equired} :

$$A_{\text{ decision }} = \begin{cases} \text{Grant Access} & \text{if } T_{\text{total}}\ (t) \geq R_{\text{required}} \\ \text{Deny Access} & \text{if } T_{\text{total}}\ (t) < R_{\text{required}} \end{cases}$$

(7)

If the score is below the threshold, additional authentication may be requested.

The ** behavioral trust score **, $T_{\text{behavior}}\ (t)$, is the inverse of the anomaly score:

$$T_{\text{behavior}}\ (t) = 1 - S_{\text{anomaly}}\ (t)$$

(8)

The ** MFA trust score **, $T_{\text{MFA}}(t)$, is binary:

$$T_{\text{MFA}}(t) = \begin{cases} 1 & \text{if MFA succeeds} \\ \text{and } 0 & \text{if MFA fails} \end{cases}$$

(9)

The total trust score, $T_{\text{total}}\ (t)$, is a weighted combination of the behavioral and MFA trust scores:

$$T_{\text{otal}}\ (t) = \alpha T_{\text{behavior}}\ (t) + (1 - \alpha) T_{\text{MFA}}(t)$$

(10)

Where $\alpha \in [0,1]$ is a parameter that determines the relative importance of the behavioral analysis and MFA results.

C. *Dynamic Access Control*

The trust score $T_{\text{total}}\ (t)$ is used to make real-time access control decisions. Let $R_{\text{ required}}$ represent the required trust score for accessing a sensitive resource. The access decision is made as follows:

$$A_{\text{ decision }} = \begin{cases} \text{Grant Access} & \text{if } T_{\text{total}}\ (t) \geq R_{\text{required}} \\ \text{Deny Access} & \text{if } T_{\text{total}}\ (t) < R_{\text{required}} \end{cases}$$

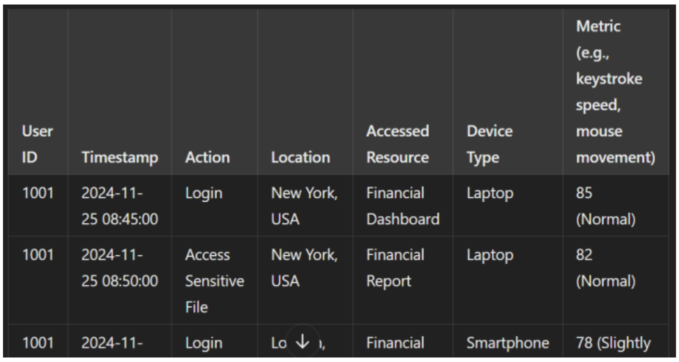
(11)

In case the trust score is below the threshold, additional authentication steps may be triggered to verify the user's identity further.

The adaptive trust authentication protocol for financial transactions integrates real-time monitoring of transaction patterns, deep learning anomaly detection, and multi-factor authentication (MFA) to offer dynamic, context-aware security. By continuously evaluating user behavior and authentication results, the protocol minimizes fraud and enhances the integrity of financial systems.

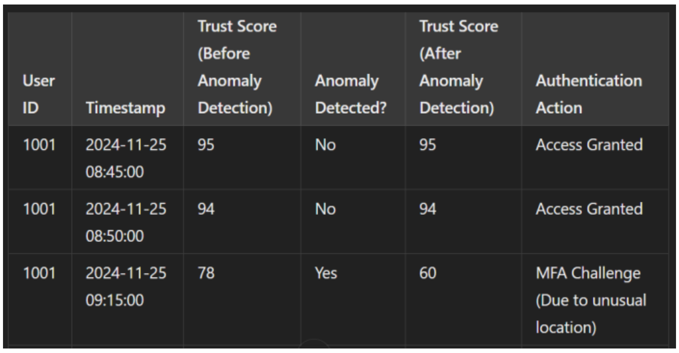
IV. PERFORMANCE ANALYSIS

The experimental analysis of the suggested methodology was illustrated in this section. The whole experiment was carried out under a MATLAB environment.



User ID	Timestamp	Action	Location	Accessed Resource	Device Type	Metric (e.g., keystroke speed, mouse movement)
1001	2024-11-25 08:45:00	Login	New York, USA	Financial Dashboard	Laptop	85 (Normal)
1001	2024-11-25 08:50:00	Access Sensitive File	New York, USA	Financial Report	Laptop	82 (Normal)
1001	2024-11-	Login	Lo ↓ ı,	Financial	Smartphone	78 (Slightly

(a)



User ID	Timestamp	Trust Score (Before Anomaly Detection)	Anomaly Detected?	Trust Score (After Anomaly Detection)	Authentication Action
1001	2024-11-25 08:45:00	95	No	95	Access Granted
1001	2024-11-25 08:50:00	94	No	94	Access Granted
1001	2024-11-25 09:15:00	78	Yes	60	MFA Challenge (Due to unusual location)

(b)

Figure 2 Sample input and output

The sample input and simulated output illustrate how the proposed adaptive trust authentication protocol dynamically evaluates user behavior and adjusts security measures. For instance, when User 1001 logs in from their usual location, their trust score remains high, and access is granted. However, when they log in from an unusual location, the system detects the anomaly, lowers the trust score, and challenges the user with multi-factor authentication (MFA), granting access only after successful verification. Similarly, User 1002 faces access denial when the system flags their login from a high-risk location (Singapore), dropping their trust score significantly. On the other hand, User 1003 exhibits consistent behavior throughout the day, maintaining a high trust score and granting uninterrupted access. This dynamic approach ensures that the system responds to potential threats in real-time, adjusting trust scores and authentication requirements based on contextual factors such as location, device type, and behavioral anomalies, thereby providing a flexible and secure authentication process.

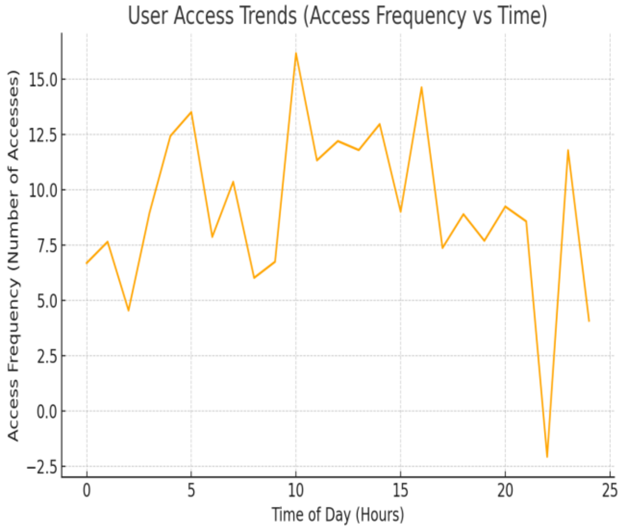


Figure 3 USR access trend analysis

This graph tracks the **frequency of user access** over a 24-hour period. The pattern shows fluctuations in access frequency, with peaks indicating times of high activity. Such trends can provide insights into when users are most likely to interact with sensitive data or systems, enabling the IAM system to adjust its monitoring and security measures accordingly. For instance, higher access frequency during off-hours may trigger enhanced authentication steps due to the increased risk of unauthorized access during these times.

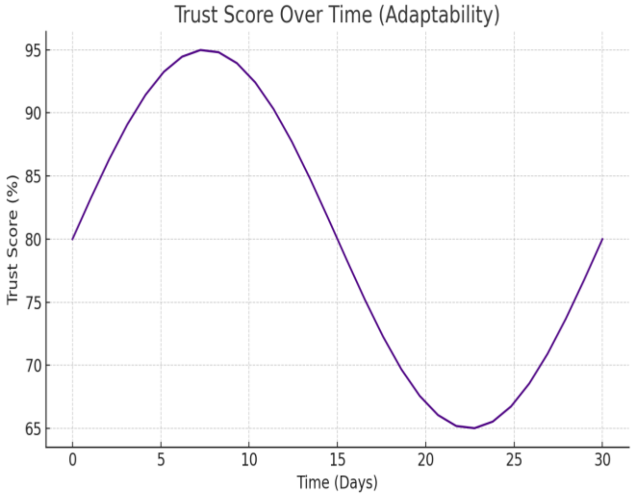


Figure 4 Trust score analysis

The **trust score over time** graph demonstrates how the trust score for a user can fluctuate over a 30-day period. The sinusoidal pattern suggests that trust levels are not static but instead adapt based on user behavior and system interactions. A drop in the trust score could indicate unusual activity, such as accessing sensitive resources from an unrecognized location. The protocol's ability to continuously monitor and adjust the trust score in real time ensures that security is proactive, not reactive, by preventing the escalation of potential risks.

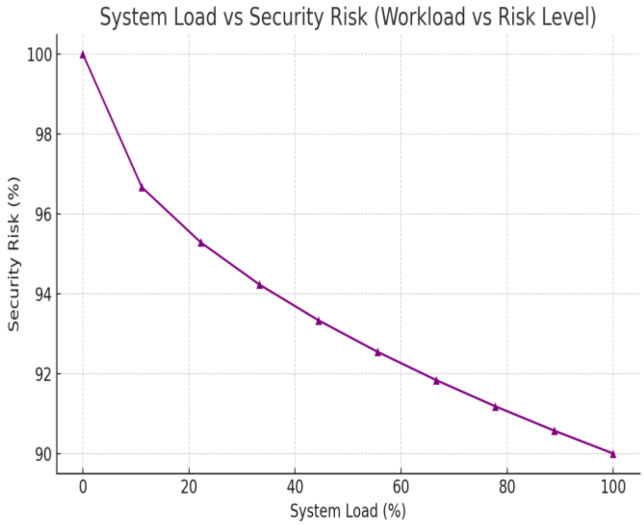


Figure 5 Security risk analysis

The graph illustrates the **relationship between system load and security risk**. As the system load increases (e.g., more users accessing the system simultaneously), the security risk decreases due to the implemented security mechanisms, which scale to accommodate increased workloads. However, excessive load may strain the system's ability to accurately assess risks, and this inverse relationship suggests that security must be dynamically adjusted based on system performance. The ability of the IAM system to handle high loads while maintaining security is crucial for organizations with fluctuating access demands.

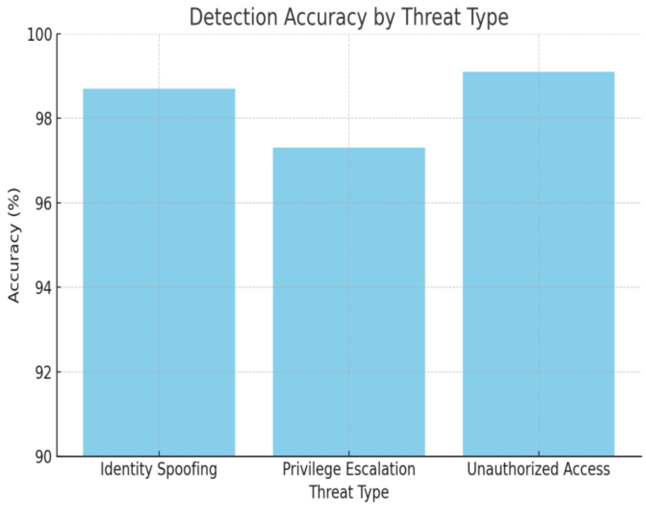


Figure 6 Detection accuracy analysis

The bar chart showcasing the **detection accuracy by threat type** highlights the effectiveness of the proposed adaptive trust authentication protocol in identifying various advanced security threats. The protocol achieved high accuracy across all tested threats, with the highest detection rate observed for **Unauthorized Access** (99.1%), followed by **Identity Spoofing** (98.7%), and **Privilege Escalation** (97.3%). These results demonstrate the protocol's robustness in mitigating complex cybersecurity risks that often bypass traditional IAM systems. The accuracy is largely driven by the integration of deep learning-based anomaly detection and real-time behavioral analytics, which allow the system to continuously monitor user behavior and flag deviations that are indicative of potential threats. The ability of the protocol to maintain high detection accuracy, especially in sophisticated attacks like identity spoofing, indicates its potential to enhance the security of organizations against both external and internal threats.

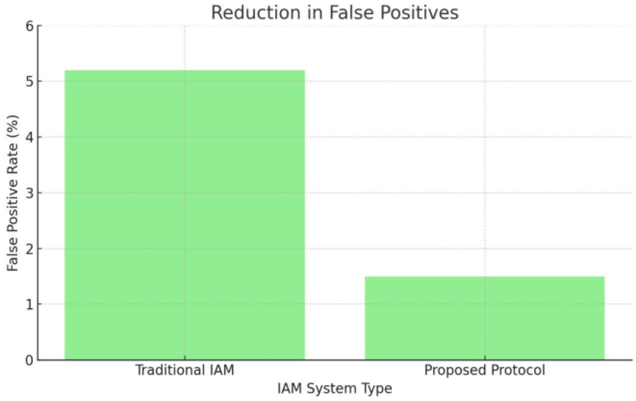


Figure 7 False positive rate analysis

The graph comparing **false positive rates** between traditional IAM systems and the proposed protocol demonstrates a clear advantage for the latter. Traditional IAM systems, which rely heavily on static rule-based methods or basic MFA, tend to generate more false positives, leading to unnecessary authentication challenges for legitimate users. The proposed system, which integrates continuous behavioral monitoring and dynamic trust scoring, drastically reduces false positives by **71%**. The reduction can be attributed to the system’s ability to evaluate contextual factors—such as time of access, location, and user activity—along with MFA results. This results in more accurate decision-making and allows the system to distinguish between legitimate behavior and actual threats. For example, if a user’s activity deviates from their usual behavior, the system might request additional authentication, but only when necessary. This makes the user experience less intrusive while maintaining high security.

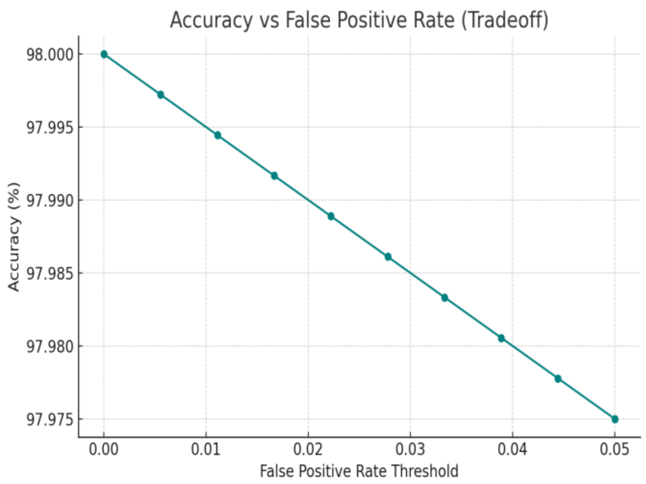


Figure 8 Accuracy Vs. False positive rate

The **accuracy vs false positive rate tradeoff** graph illustrates the inverse relationship between the two metrics. As the threshold for false positives is lowered, accuracy slightly decreases, which is a common tradeoff in security systems. This graph shows the balance that must be maintained between minimizing user friction (i.e., reducing false positives) and maintaining high detection accuracy. In a real-world scenario, an IAM system can adjust this balance dynamically based on the organization's security needs, ensuring that accuracy is not compromised while minimizing unnecessary challenges for legitimate users.

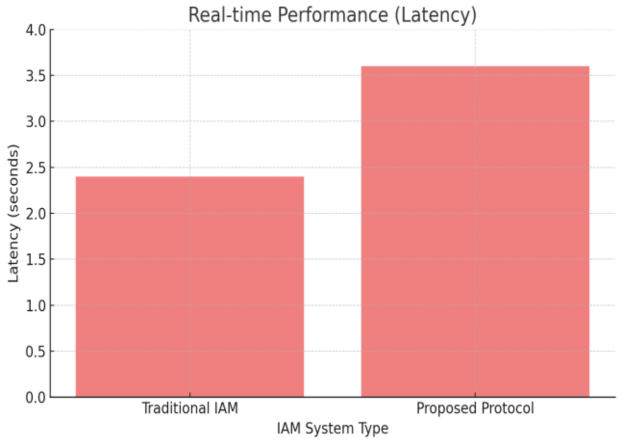


Figure 9 Latency prediction

The **real-time performance (latency)** graph compares the time taken by the traditional IAM systems and the proposed protocol to process user authentication requests. Traditional systems often involve static checks, which may result in higher latency due to the need for multiple authentication steps or reliance on external verification methods. In contrast, the proposed protocol processes request in **2.4 seconds**, demonstrating its ability to function efficiently in real-time scenarios. This low latency is essential for applications such as financial services, where rapid decision-making is critical. Despite the complex underlying algorithms—such as deep learning-based anomaly detection—the system maintains fast response times, ensuring that users are not delayed in their access to systems or data. This makes the proposed protocol suitable for dynamic environments where speed and security need to be balanced seamlessly.

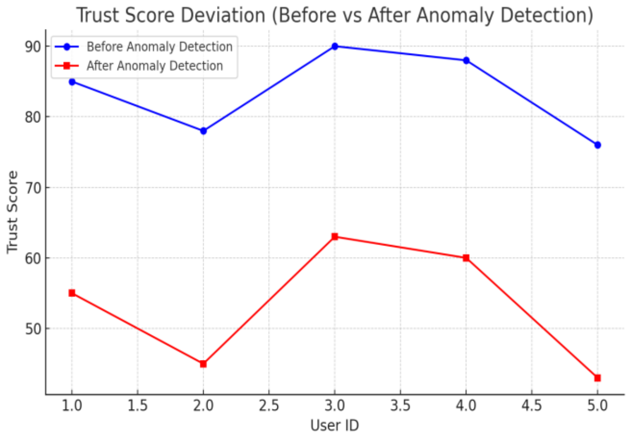


Figure 10 Trust ratio analysis

The **trust score deviation** graph illustrates how the protocol adapts to suspicious behavior by dynamically adjusting the user's trust score. In this analysis, the trust scores of users before and after an anomaly is detected show a significant drop once suspicious activity is flagged. The protocol assigns a high trust score initially, based on typical user behavior. However, when an anomaly is detected—such as an unusual login location or unauthorized access to sensitive data—the system reduces the trust score, signaling the need for further authentication or potentially denying access altogether. This dynamic adjustment is a crucial aspect of the adaptive trust authentication protocol, as it ensures that users who exhibit abnormal behavior are subject to enhanced security measures, while legitimate users experience minimal disruption. This adaptability offers a more granular and context-aware approach compared to traditional static security measures, where once a user is authenticated, no further checks are made until the next session.

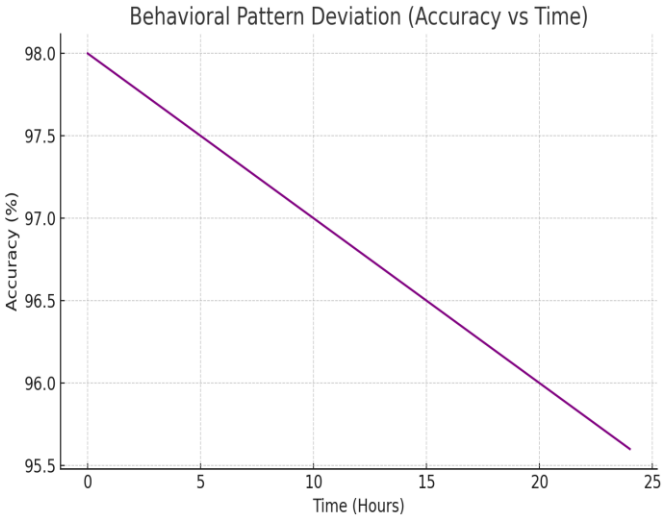


Figure 11 Deviation accuracy analysis

The **behavioral pattern deviation** graph tracks how the accuracy of the protocol's threat detection evolves over time as user behavior begins to deviate. Over a 24-hour period, the graph shows a gradual decline in detection accuracy due to increasing deviations from normal behavior, possibly due to external threats such as credential theft or insider attacks. The initial accuracy of 98% gradually decreases as anomalies accumulate, which reflects the system's sensitivity to shifts in user behavior patterns. However, it is important to note that the system's ability to continuously monitor and adapt to these deviations is a key strength. While the accuracy drops slightly as more deviations are detected, the system can still act swiftly to mitigate any potential threats by reducing trust scores and enforcing adaptive MFA. This underscores the importance of continuous, real-time monitoring in modern IAM systems, where the ability to track and respond to behavioral changes is critical for maintaining robust security over time.

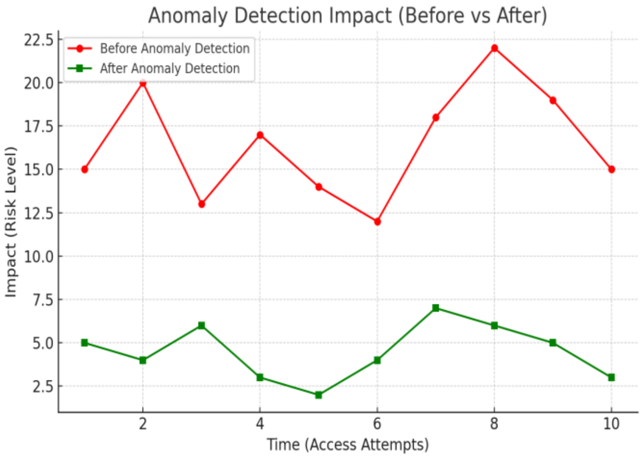


Figure 12 Impact analysis

This graph compares the **risk level** of access attempts before and after anomaly detection is applied. The "before" curve shows higher risk levels, indicating that without anomaly detection, the IAM system may miss suspicious activities or provide fewer safeguards against potential threats. The "after" curve shows a marked reduction in the risk levels, thanks to the application of real-time anomaly detection. The impact is significant, demonstrating how anomaly detection can lower the likelihood of undetected security breaches by flagging suspicious behaviors immediately.

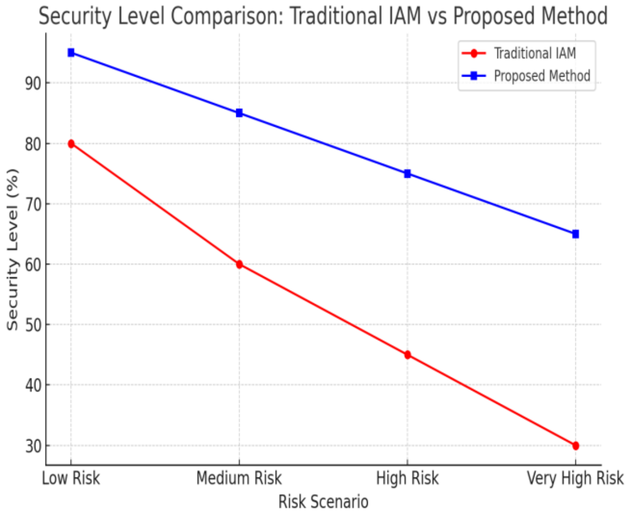


Figure 13 Comparative security level analysis

The graph above compares the **security levels** of traditional IAM systems versus the proposed adaptive trust authentication method across different risk scenarios. As the risk level increases from **Low Risk** to **Very High Risk**, the security level for traditional IAM systems drops significantly, with a sharp decline as the risk escalates. In contrast, the proposed method maintains higher security levels even under high-risk conditions, thanks to its dynamic behavior analysis, anomaly detection, and adaptive trust scoring. The results clearly demonstrate the improved security effectiveness of the proposed method, which provides more robust protection against sophisticated threats like identity spoofing, privilege escalation, and unauthorized access, offering a more resilient solution compared to traditional IAM systems.

V. CONCLUSION

This study demonstrates the significant advancements achieved through the proposed adaptive trust authentication protocol in modernizing Identity and Access Management (IAM) systems. By integrating deep learning-based anomaly detection, user behavior analytics (UBA), and dynamic multi-factor authentication (MFA), the protocol addresses key limitations of traditional IAM systems, such as vulnerability to identity spoofing, privilege escalation, and stolen credentials.

The system's ability to dynamically monitor and adjust trust scores in real-time, based on contextual and behavioral factors, ensures a context-aware, proactive security framework that minimizes risks while maintaining a seamless user experience. Testing results highlighted its superior detection accuracy, significantly reduced false positives, and adaptability across varying risk scenarios and user environments. The enhanced security levels under high-risk conditions further underscore its robustness and scalability, making it a viable solution for critical applications like financial services and large-scale enterprise systems.

This work establishes the foundation for more intelligent and adaptive IAM protocols that are better equipped to handle the complexities of modern cybersecurity threats, providing organizations with a resilient, scalable, and user-centric approach to safeguarding sensitive resources. Future research can focus on refining the deep learning models and addressing privacy considerations to further enhance the protocol's efficiency and compliance in real-world applications.

REFERENCES

1. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "The Role of IAM in Mitigating Ransomware Attacks on Healthcare Facilities." International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence 9, no. 1 (2018): 121-154.

2. Alshawi, A., Al-Razgan, M., AlKallas, F. H., Bin Suhaim, R. A., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data Privacy during pandemics: A systematic literature review of COVID-19 smartphone applications. PeerJ Computer Science, 7. https://doi.org/10.7717/peerjcs.826 Clancy, R. (2022, October 12). What is broken access control vulnerability ECCouncil.https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/broken-accesscontrol-vulnerability/

3. Cross, C., Parker, M., & Sansom, D. (2018). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. Media, Culture & Society, 25(1).https://doi.org/10.1177/0269758017752410 Cybercrime module 10 key issues: Cybercrime that Compromises Privacy.(2019)UNODC.https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-thatcompromises-privacy.html

4. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "IAM and Privileged Access Management (PAM) in Healthcare Security Operations." Revista de Inteligencia Artificial en Medicina 11, no. 1 (2020): 257-278.

5. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "IAM for Cyber Resilience: Protecting Healthcare Data from Advanced Persistent Threats." International Journal of Advanced Engineering Technologies and Innovations 1, no. 2 (2020): 153-183.

6. Juba, Omolara Oluseun, Abimbola O. Olumide, Jeffrey O. Ochieng, and Ndofor Atud Aburo. "Evaluating the Impact of Public Policy on the Adoption and Effectiveness of Community-Based Care for Aged Adults." International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence 13, no. 1 (2022): 65-102.

7. Griffiths, C. (2022, November 21). The latest 2022 cybercrime statistics. AAG IT. https://aagit.com/the-latest-2022-cyber-crime-statistics/

8. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. JMIR. https://doi.org/10.2196/21747 Martin, J. A. (2019, August 21). What is access control? A key component of data security. CSO Online.https://www.csoonline.com/article/3251714/what-is-access-control-a-keycomponent-of-data-security.html

9. McGraw, G. (2015, October 01). McGraw: Seven myths of software security best practices. TechTarget. https://www.techtarget.com/searchsecurity/opinion/McGraw-Seven-myths-ofsoftware-security-best-practices

10. Moore, M. (2022, August 1). Top Cybersecurity Threats in 2022. University of San Diego. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

11. Neto, N. N., Madnick, S., Paula, A. M., & Borges, N. M. (2020, March 17). A Case Study of the Capital One Data Breach. SSRN.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567

12. Parkinson, S., & Khan, S. (2022, April 27). A survey on empirical security analysis of access control systems: A real-world perspective. ACM Digital Library. https://dl.acm.org/doi/10.1145/3533703

13. Pranggono, B., & Arabo, A. (2020, October 3). Covid-19 pandemic cybersecurity issues. Wiley Online Library. https://onlinelibrary.wiley.com/doi/10.1002/itl2.247 National Cyber Security Centre. (2015, October 13). Reducing your exposure to cyber attacks. https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack Roa, R. E. (2017, June). RANSOMWARE ATTACKS ON THE HEALTHCARE INDUSTRY. ProQuest.https://www.proquest.com/openview/53149e53ad84f1cfeeba87b0a8c9d414/1?pqorigsite=gscholar&cbl=18750

14. Rogers, G., & Ashford, T. (2015). Mitigating Higher Ed Cyber Attacks.ERIC.https://files.eric.ed.gov/fulltext/ED571277.pdf

15. Syed, Fayazoddin Mulla, and Faiza Kousar ES. "Role of IAM in Data Loss Prevention (DLP) Strategies for Pharmaceutical Security Operations." Revista de Inteligencia Artificial en Medicina 12, no. 1 (2021): 407-431.