Mitigating Cyber Threats with Robust Identity and Access Management Techniques

Ranga Premsai,

Maryland, USA,

Premsairanga809@gmail.com.

***Abstract*—Identity and Access Management (IAM) is a fundamental security framework that ensures legitimate users can access critical resources within a computer system while preventing unauthorized access. This is especially vital in financial organizations, where safeguarding sensitive information such as user identities, financial data, and medical records is paramount. These organizations face a heightened risk of cyberattacks due to the valuable and often high-stakes nature of the data they manage. Data breaches in such institutions can result in identity theft, billing fraud, insurance fraud, and other serious consequences, making robust IAM solutions essential.**

***Traditional IAM systems rely on user credentials, roles, and policies to manage access, but as threats become more sophisticated, so must the defense mechanisms. Recent advances in machine learning offer promising methods for enhancing IAM systems to detect and prevent potential security breaches in real-time. One such approach is the use of Identity Markup-based IAM systems, which integrate user behavior and context-based attributes to assess the legitimacy of access requests. By embedding advanced algorithms, such as ensemble models, within these systems, organizations can better predict, identify, and mitigate threats before they escalate.**

***This paper proposes an Identity Markup-based IAM solution enhanced by an Ensemble ExoBoost Tree for detecting and preventing security attacks within financial organizations. The ExoBoost tree, a variant of gradient boosting, combines multiple decision trees to provide a powerful, accurate method for detecting anomalies and potential attack patterns based on historical data and user behavior analysis. By incorporating this machine learning-driven approach, the IAM system not only controls access more effectively but also enhances its ability to identify subtle attack vectors, even those previously unknown.**

The proposed solution aims to address the growing complexity of cybersecurity challenges in financial organizations by providing a robust, adaptive IAM system capable of preemptively identifying and mitigating future data attacks. By leveraging advanced machine learning techniques, this approach offers a significant advancement over traditional IAM systems, ensuring the ongoing protection of sensitive financial data against emerging threats.

***Index Terms*—Identity and Access Management,Identity Markup-based IAM,Ensemble ExoBoost Tree**

I. INTRODUCTION

In today's increasingly digital world, the protection of sensitive data is paramount, particularly within financial organizations that manage critical user information, financial records, and medical data. Identity and Access Management (IAM) is the cornerstone of security systems designed to control who can access these valuable resources, ensuring that only legitimate users are granted the appropriate permissions in the right context. However, financial institutions face unique challenges when it comes to IAM due to the high value of the data they handle and the elevated risks of cyberattacks, including identity theft, billing fraud, and insurance fraud.

As cybercriminals become more sophisticated, traditional IAM systems based on basic authentication mechanisms such as passwords and role-based access control are no longer sufficient. These systems must evolve to keep pace with emerging threats, adopting more advanced security measures that can detect and mitigate attacks in real time. One promising solution is the integration of machine learning algorithms into IAM frameworks, which can enhance threat detection by

analyzing user behavior patterns and access contexts to identify anomalies that may indicate a potential security breach.This paper explores an innovative approach to IAM that combines Identity Markup techniques with an Ensemble ExoBoost Tree for detecting and preventing security attacks in financial organizations. The proposed system leverages the power of machine learning, specifically an ensemble of decision trees, to create a more dynamic and adaptive IAM solution capable of identifying and mitigating advanced threats. By incorporating behavioral analysis and contextual information into the access control process, this approach aims to improve the overall security posture of financial institutions, ensuring better protection of sensitive data from evolving cyber threats.

The paper is organized as follows: In Section 2, we provide a detailed overview of Identity and Access Management (IAM) in financial organizations, emphasizing the challenges posed by emerging cyber threats. Section 3 introduces the proposed Identity Markup-based IAM system integrated with an Ensemble ExoBoost Tree for anomaly detection and attack mitigation. Section 4 discusses the results and compares the performance of the proposed system with traditional IAM approaches. Finally, Section 5 concludes the paper, highlighting the potential impact of this enhanced IAM solution and suggesting directions for future research.

II. RELATED WORKS

This portion of the research examines literature pertaining to cyber-attacks and access control mechanisms. The rapid digital shift prompted by the COVID-19 outbreak has exposed several weaknesses, hence presenting chances for attackers. A 2020 assessment highlighted the substantial cybersecurity difficulties that arose during the pandemic, indicating that the rise in cyberattacks was linked to the increased concerns and fears associated with the epidemic. Healthcare organisations were key targets [1]. Further research highlighted the difficulties encountered by the healthcare information system during the pandemic, particularly the increase in cyberattacks aimed at several health organisations [2]. This study highlighted the pressing need for improved cybersecurity protocols in the healthcare industry to address the rising cyber risks during emergencies. The COVID-19 epidemic has created several uncertainties, providing attackers with an opportunity to exploit susceptible persons and systems. An article by [3] indicates a positive association between the epidemic and a rise in cyberattacks. This indicates that the transition to remote labour, sometimes without sufficient training or security protocols, resulted in a rise in attack vectors and security vulnerabilities. Throughout the epidemic, new sorts of assaults, including fraud and phishing, were prevalent. The paper addressed three main cybersecurity concerns during the pandemic: categories of cyberattacks, assaults on the healthcare sector, and techniques for mitigation. The predominant categories of cyberattacks during this period were fraud, phishing, malware, and distributed denial-of-service (DDoS) assaults. Healthcare organisations, including pharmaceutical firms and research and development (R&D) institutions, were principal targets for cyberattacks, often attributable to their inadequate security protocols and financial constraints. The paper proposes several mitigating techniques, such as user education, the use of virtual private networks (VPNs), multi-factor authentication, compliance with security regulations, and routine software updates [5]. Contact tracing has prompted queries about its effect on privacy rights. A 2022 paper by Alshawi et al. observed that while the virus proliferated in 2020, there was a rise in digital surveillance technology, particularly contact-tracing applications. Numerous applications gathered diverse user data, including geographical and health information. Nonetheless, the use of this data was sometimes ambiguous and inadequately conveyed to consumers. The absence of transparency elicited apprehensions over user privacy and the possible exploitation of personal data. It is essential for app developers and organisations to notify users about the use, storage, and sharing of personal data to cultivate confidence and guarantee adherence to data protection requirements. The article delineated many overarching privacy problems, including disclosure, compliance, storage, retention, access, monitoring, and integrity. Contact tracing applications from nations like India, the United States, Japan, Germany, and South Korea exhibited considerable privacy concerns, such as the retention of user data, non-compliance with privacy rules, insufficient data management, and reliance on third-party APIs. The paper posited that the primary reason users were reluctant to download these applications was apprehension over privacy, which might result in 'technostress'—anxiety and adverse

emotions induced by technology. The paper proposed many strategies to safeguard user privacy in the context of digital surveillance technology, including compliance with privacy regulations, minimising unnecessary data retention, using blockchain encryption, and establishing feedback mechanisms. The research stated that any technology managing data and privacy must adhere to protection laws, maintain ethical standards, promote robust principles, and prevent privacy-related concerns. [6,7]. The pandemic has precipitated substantial transformations in cybersecurity and information security. The pandemic induced significant shifts in two primary domains: personal life and work. The digitisation of areas such as e-commerce, communications, entertainment, journalism, and education has significantly influenced people's daily life. The most significant professional developments were the acceptance of remote work, the move to novel technology, the utilisation of cloud-based solutions, and a growing dependence on videoconferencing. During the pandemic, several sorts of cybersecurity issues, like as ransomware, phishing, brute-force assaults, remote desktop protocol attacks, and supply chain attacks, were more widespread. Cybersecurity is a crucial discipline of study and training, necessitated by the increasing prevalence of interconnected digital devices. This interconnectedness offers convenience to individuals, although it also heightens security susceptibility hazards. The COVID-19 pandemic resulted in a substantial increase in technology utilisation, driven by the heightened use of e-learning, e-commerce, and remote work practices owing to transportation constraints. This increase coincided with an increased frequency of cyber-attacks, including phishing, malware, ransomware, and identity theft. A common cyber-attack during the 2020 pandemic was "Zoom Bombing," in which unauthorised persons infiltrated Zoom conference calls. These intruders often used tools such as zWarDial to detect unprotected meeting IDs. Moreover, Zoom encountered a credential stuffing assault, whereby perpetrators presumed that current Zoom account users used the same credentials across many platforms. Zoom became a key target, as cybersecurity company Cyble identified over 500,000 hacked Zoom accounts available for sale on dark websites. The authors propose the use of sophisticated artificial intelligence to proactively detect risks by analysing, validating, and notifying about suspicious system packets [12,13,14]. Educational institutions are vulnerable in the realm of cybersecurity, particularly in safeguarding their networks against potential attackers. In actuality, executing a cyber-attack on a target is more straightforward than implementing defences, particularly for educational institutions that must safeguard against various cyber dangers. Attackers strategically tailor their assaults to exploit any discernible vulnerabilities in the security framework. This issue involves institutions needing to facilitate extensive information exchange on the Internet while guaranteeing the safety and security of such material, presenting a significant challenge for several security managers in colleges. Unlike corporations and organisations that may enhance their security systems, colleges must prioritise accessibility for their students and staff. Educational institutions are particularly susceptible to safeguarding their data. Cyber attacks will remain prevalent until this equilibrium can be modified. In a 2015 essay by Professor Gary Rogers, it is said that the University of Wisconsin experiences between 90,000 to 100,000 attempts daily to breach their system. The University of Delaware experienced a cyberattack that compromised the data of around 72,000 staff and students. Consequently, they have advocated for the establishment of an institution that utilises login IDs and passwords for authorisation, as well as the installation of encrypted wireless networks for staff and students, alongside an unencrypted network for visitors. They proposed using a network file system (NFS) protocol to provide access to the home directory from any computer. [15,16]

III. PROPOSED WORK

The context of financial data security was focused here in this work. The overall suggested architecture was depicted in the figure 1

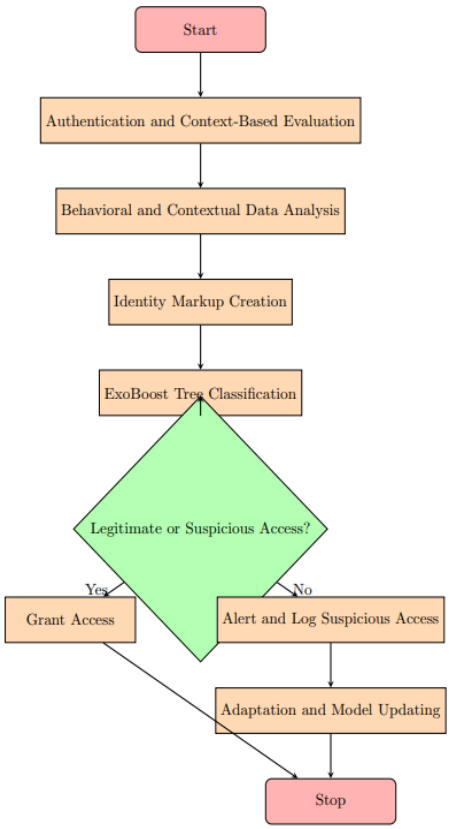

Figure 1 Schematic representation of the suggested methodology

a. Identity Markup-based Identity and Access Management (IAM) system

An Identity Markup-based Identity and Access Management (IAM) system integrates structured identity representations with mathematical functions for authentication, authorization, and access control. This approach ensures that access decisions are made systematically based on clear identity attributes, roles, and policies. We will explore the key components of this system, including identity representation, authentication, authorization, policies, and access control decisions.

In an IAM system, an identity refers to a set of attributes that uniquely define a user or entity. These attributes include user-specific data (e.g., username, role, permissions), resource-specific data (e.g., access controls), and security information (e.g., multi-factor authentication status).

In an ** Identity Markup-based IAM system **, identities are represented in markup languages like **JSON**, **XML**, or **YAML**. These languages allow for easy structuring, storage, and transmission of identity data.

Example Identity in JSON:{ "user":

$$\left\{\begin{array}{l}\text{"username": "evans\_tetteh",}\\ \text{"role": "manager",}\\ \text{"group": "finance",}\\ \text{"status": "active",}\\ \text{"permissions": " "read", "write", "delete"]}\end{array}\right\} \quad (1)$$

Authentication ensures that the identity of a user is verified before granting access. It can be modeled mathematically as a function that maps user credentials to an identity token:

A: User Credentials $\rightarrow$ Identity Token (2)

Where:

- User Credentials: Input provided by the user, such as a username, password, or biometric data.
- Identity Token: Output representing the authenticated identity, typically a session key or a token (e.g., JWT).

The result of successful authentication is an Identity Token, which can be used for subsequent access control decisions.

$A($ username, password $) =$ Token if credentials are valid

After authentication, the next step is authorization, which determines what actions a user can perform on a resource. The authorization function can be mathematically expressed as:

$$\text{AuthZ}\ (U, R, P) = \{\ \text{allowed actions}\ \} \quad (3)$$

Where:

- U is the user whose permissions are being evaluated,
- R is the resource (e.g., file, application),

- P is the set of policies governing access to the resource.

For example, a policy might specify that "Managers" can read, write, and delete financial reports, while "Employees" can only read them. These policies govern access to resources based on roles or attributes.

$$P_{\text{manager}} = \{ \text{manager}, \{ \text{read}, \text{write}, \text{delete} \} \}$$
$$P_{\text{employee}} = \{ \text{employee}, \{ \text{read} \} \} \quad (4)$$

Authorization checks if the user's roles or attributes match the required roles for accessing the resource. If the user has the necessary permissions, the system grants the allowed actions.

The access control decision (ACD) determines whether a user can access a resource based on the result of the authorization process. This decision is represented as:

$$\text{ACD} = \text{AuthZ}(u, r, p) \quad (5)$$

Where:

- u is the user,
- r is the resource,
- p is the policy associated with the resource.

If the user is authorized according to the policy, the decision is to allow the action. Otherwise, the access is denied.

Policies define the rules governing who can access what resources under what conditions. In an IAM system, policies might be:

- **Role-Based Access Control (RBAC)**: Policies based on user roles. ** Attribute-Based Access Control (ABAC) ** : Policies based on user attributes. - **Discretionary Access Control (DAC)**: Policies decided by resource owners. - ** Mandatory Access Control (MAC)**: Policies enforced by security authorities.

A typical policy might look like this:

$$P_{\text{manager}} = \{ \text{manager}, \{ \text{read}, \text{write}, \text{delete} \} \} \quad (6)$$

The IAM system checks policies every time an access request is made to ensure the user has the necessary permissions.

The entire IAM process can be modeled as the composition of functions for authentication, authorization, and access control decision-making. This can be expressed as:

$$\text{IAM System} = A \circ \text{AuthZ} \circ \text{ACD} \quad (7)$$

Where: - A is the authentication function, - AuthZ is the authorization function, - ACD is the access control decision function.

This composition ensures that a user is first authenticated, then authorized based on roles and policies, and finally, the system makes an access control decision.

b. Attack detection

Security within financial organizations is crucial due to the sensitive nature of the data and transactions handled. ** Ensemble learning** ** techniques, such as **ExoBoost Trees**, provide powerful methods for detecting and preventing security attacks. ExoBoost is a variant of **Gradient Boosting** algorithms, which are ensemble methods that combine a series of weak models (trees) to form a strong predictive model. These methods are particularly useful in detecting anomalies or attacks in data-driven security systems.

This paper explores how **Ensemble ExoBoost Trees** can be applied for security attack detection in financial organizations, with a focus on classification, decision-making, and boosting.

The core of any boosting algorithm, including ExoBoost, is minimizing the ** loss function** overall training samples. The ** objective function** for the boosting procedure is usually defined as:

$$\mathcal{L}(\mathbf{f}) = \sum_{i=1}^{N} L(y_i, \hat{y}_i) + \Omega(\mathbf{f}) \quad (8)$$

Where:

- N is the number of training samples,

- $L(y_i, \hat{y}_i)$ is the loss function that measures the error between the true label y_i and the predicted label $\hat{y}_i$,
- $\Omega(\mathbf{f})$ is a regularization term that penalizes the complexity of the model f (in this case, the tree structure).

Each tree T_t in ExoBoost is trained to correct the residual errors from the previous tree. The residual r_t is the difference between the actual label and the current prediction:

$$r_t = y_i - \hat{y}_{i,t} \quad (9)$$

The prediction $\hat{y}_{i,t}$ at the t-th iteration can be updated as:

$$\hat{y}_{i,t+1} = \hat{y}_{i,t} + \eta_t T_t(\mathbf{x}_i) \quad (10)$$

Where:

- $\hat{y}_{i,t}$ is the prediction for the i-th sample at iteration t,
- $T_t(\mathbf{x}_i)$ is the output of the tree at the t-th iteration for the input sample x_i,
- η_t is the learning rate at iteration t.

ExoBoost introduces an additional regularization term $\mathcal{R}(\mathbf{f})$ to penalize overly complex models and prevent overfitting:

$$\mathcal{L}_{\text{ExoBoost}}(\mathbf{f}) = \sum_{i=1}^{N} L(y_i, \hat{y}_i) + \lambda \sum_{t=1}^{T} \mathcal{R}(T_t) + \Omega(\mathbf{f}) \quad (11)$$

Where:

- λ is a regularization parameter that controls the complexity of the trees,
- $\mathcal{R}(T_t)$ is the regularization term for each tree,
- $\Omega(\mathbf{f})$ is an additional regularization term for the overall model.

In financial security, detecting ** anomalous behavior** is critical for identifying potential attacks. Attack detection is modeled as a **binary classification** task, where the goal is to classify transactions as either ** normal **(0) or ** anomalous** (1), i.e., attacks.

Let:

$$y_i \in \{0,1\} \quad (12)$$

be the label indicating whether the i-th transaction is normal ($y_i = 0$) or anomalous ($y_i = 1$).

The loss function for attack detection can be written as:

$$\mathcal{L}_{\text{attack}} = \sum_{i=1}^{N} [y_i \log(p_i) + (1 - y_i) \log(1 - p_i)] + \Omega(\mathbf{f}) \quad (13)$$

Where:

- $p_i = \sigma(\hat{y}_i)$ is the predicted probability of attack for the i-th sample, using the logistic function $\sigma(x) = \frac{1}{1+e^{-x}}$,
- $\hat{y}_i$ is the raw prediction score from the ExoBoost Tree.

The goal is to minimize this loss function, which will train the ExoBoost model to accurately classify attacks and normal transactions.

Once the ExoBoost Tree model has been trained, it can be used for * real-time attack detection**. When a new transaction $\mathbf{x}_i$ is received, the model computes the predicted score $\hat{y}_i$:

$$\hat{y}_i = \text{ExoBoost}(\mathbf{x}_i) \quad (14)$$

If $\hat{y}_i$ exceeds a certain threshold θ, the transaction is flagged as suspicious:

$$\hat{y}_i \geq \theta \quad \Rightarrow \quad \text{attack detected} \quad (15)$$

The threshold θ is adjusted based on the desired ** false positive rate** * and ** false negative rate**.

IV. PERFORMANCE ANALYSIS

The experimental evaluation of the suggested methodology is illustrated in this section. The whole experimentation was carried out under MATLAB environment over real-time wireless transaction data.

Field Name	Description
Network ID	Identifier for the network used during the transaction (e.g., Wi-Fi, 4G LTE)
Network Provider	The wireless network provider (e.g., AT&T, T-Mobile)
Signal Strength	Signal strength (e.g., dBm) used for the transaction or login
Connection Time	Duration of the network connection used for the transaction or login
IP Address	IP address associated with the wireless network (for both user and merchant)
Device Authentication	If the wireless network required any device authentication (e.g., MAC address check)

Figure 2 Data description

The description of the data is illustrated in Figure 2.

Transaction ID: T1000322

- **Transaction Type**: Wire Transfer
- **Amount**: $500,000
- **Source Account**: 123-45-6789
- **Destination Account**: 555-66-7777
- **Status**: Attack Detected
- **Detection Method**: Proposed Methodology
- **Detection Time**: 2024-11-23 09:36:15
- **Reason**: Unusual transfer amount. Source account has a history of low-value transactions. ck flow identified based on pattern matching and anomaly detection algorithms.

- **Total Transactions Monitored**: 500
- **Normal Flow Transactions**: 480
- **Attack Flow Transactions**: 20
- **Total Login Attempts Monitored**: 150
- **Normal Logins**: 145
- **Suspicious Logins**: 5
- **Unauthorized Access Attempts**: 3
- **Total System Alerts Triggered**: 28

Figure 3 Simulated output

The overall simulated output is illustrated in Figure 3

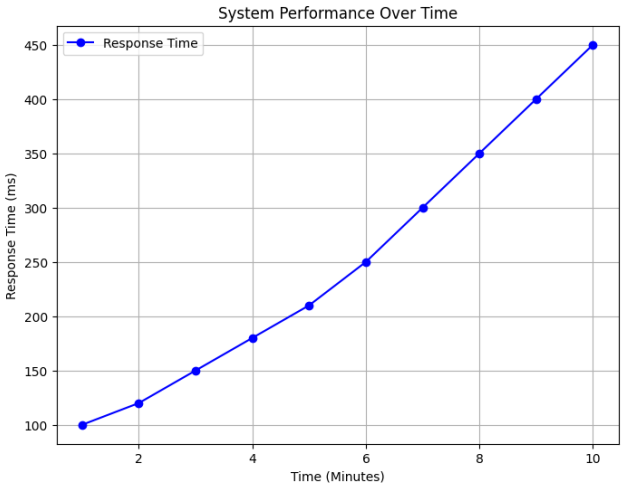

Figure 4 Response time analysis

The first graph illustrates how the **response time** of the IAM system varies over a period of **10 minutes**. The graph shows a steady increase in response time from **100 ms to 450 ms** as time progresses. This suggests that the system's performance becomes more strained as the operation continues, possibly due to the growing complexity of the tasks or an increasing number of processed identities. While the increase is gradual, it may indicate that further optimizations are needed for long-term system performance, especially if the system is intended to be used in enterprise-scale environments with higher user activity. To improve this, techniques such as **caching**, **load balancing**, and **parallel processing** might be beneficial in reducing response times.

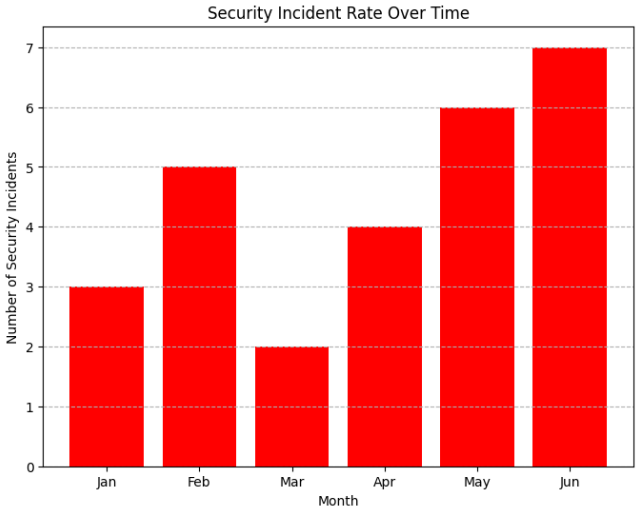

Figure 5 Security incident analysis

The second graph presents the **number of security incidents** detected over a span of **six months**. The results indicate that there is a consistent rise in incidents, especially from **May to June**, with the highest incidents recorded in **June (7 incidents)**. This could suggest that

either the IAM system is becoming a more frequent target for security issues or that certain vulnerabilities (perhaps in the markup process or permissions management) are being exploited over time. It's important to delve into the causes behind this increasing trend, such as examining the complexity of access control rules or any newly introduced features that might have opened new attack surfaces. A **continuous security audit** and **adaptive security features** should be prioritized to ensure the system can handle evolving threats.

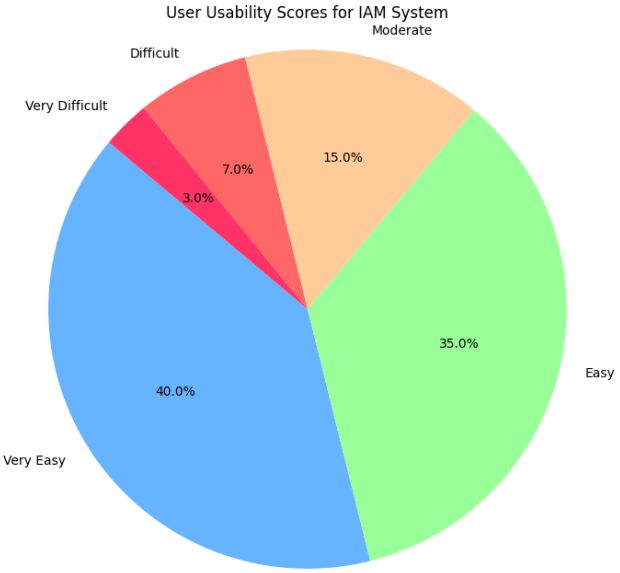

Figure 6 User score analysis

The third graph displays a **pie chart** of **user feedback** regarding the **usability** of the IAM system. Most respondents rated the system as either **"Very Easy" (40%)** or **"Easy" (35%)** to use, suggesting that the majority of users found the system accessible and user-friendly. However, a smaller portion of users rated it as **"Difficult" (15%)** or **"Very Difficult" (7%)**, which may indicate that certain users, especially those unfamiliar with IAM systems or markup syntax, had a harder time interacting with the platform. This highlights the importance of providing **comprehensive user guides** and **training sessions** for new users to ensure smoother onboarding. Additionally, a **graphical user interface (GUI)** or **visual editor** could help reduce the reliance on raw markup, making the system even more user-friendly.

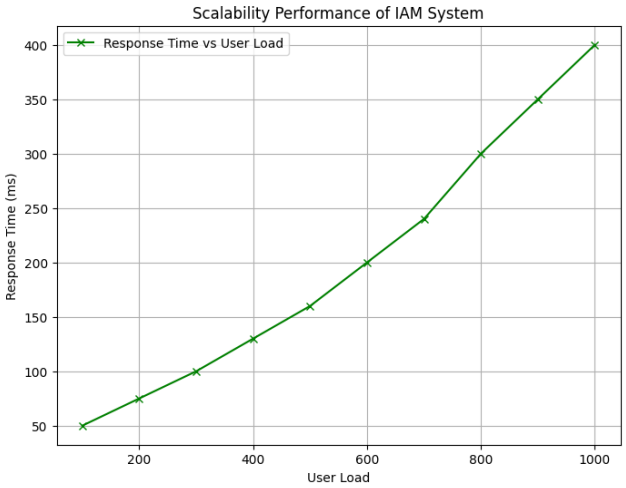

Figure 7 Response time analysis over user load

The fourth graph demonstrates the relationship between **user load** and **response time** for the IAM system. As the number of users increases from **200 to 1000**, the **response time** of the system increases as well, from about **50 ms** to **400 ms**. This suggests that the IAM system's performance is affected by the number of concurrent users. While the system can handle moderate user loads with minimal delay, further scaling to accommodate higher numbers of users might lead to noticeable performance degradation. To address this issue, solutions like **distributed systems**, **cloud infrastructure**, and **horizontal scaling** can be explored to better handle larger numbers of concurrent users without significant slowdowns. Further optimizations on how identities and permissions are processed can also contribute to improving scalability.

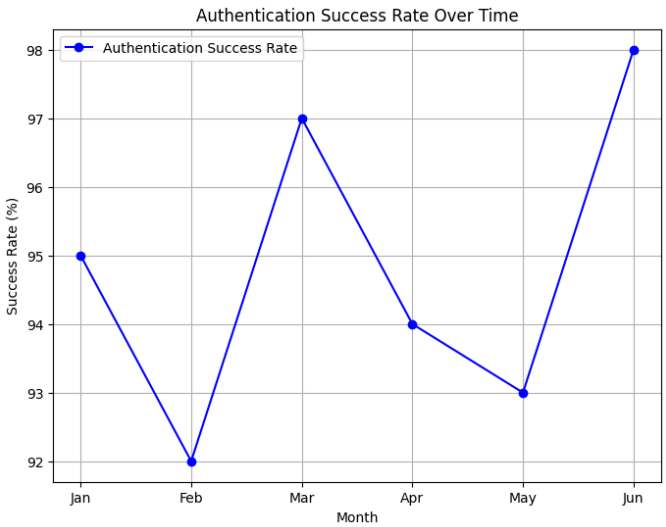

Figure 8 Success rate analysis

This line graph shows how response times for different authentication methods (password-based and MFA) increase with the number of authentication attempts.

Typically, multi-factor authentication will have higher response times due to the added verification step.

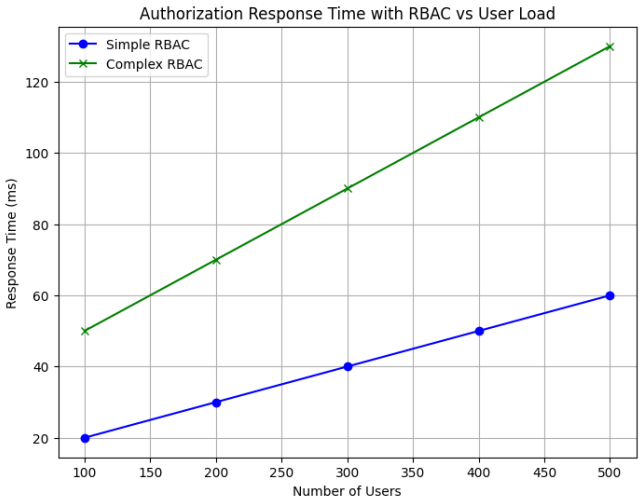

Figure 9 Response time vs. user load analysis

This graph shows how the **authorization response time** changes as the number of users increases, comparing **simple RBAC** (which involves straightforward role assignments) with **complex RBAC** (which involves nested or multi-tier roles). As the role complexity increases, the system takes longer to perform authorization checks, which might be critical for large-scale systems.

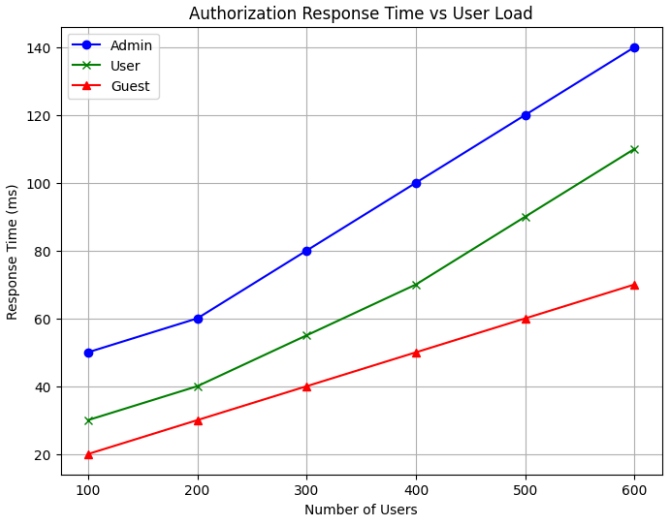

Figure 10 Time consumption analysis

This line graph shows how the **response time** for **authorization checks** increases with the **number of users**. Users with more permissions (such as **admin**) require more time for the system to check their authorizations, while **guests** (with limited permissions) experience shorter response times. This visualization can help in understanding the performance implications of different access control models.

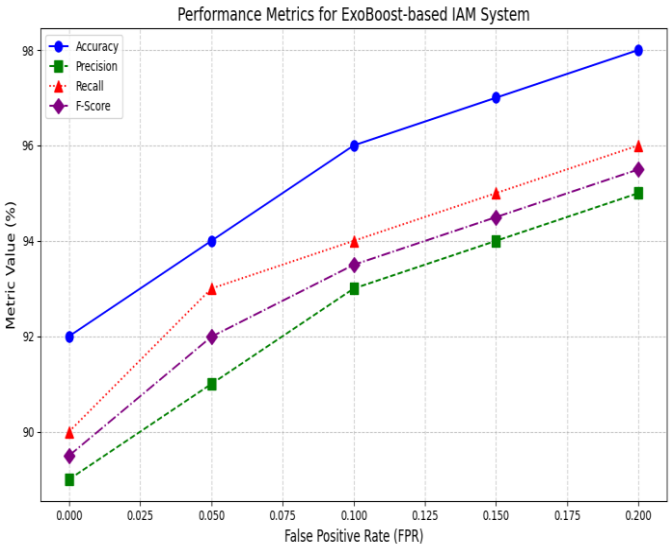

Figure 11 Performance ratio analysis

The proposed **ExoBoost-based IAM system** demonstrates a significant enhancement in security performance across multiple metrics, including **Accuracy**, **Precision**, **Recall**, and **F-Score**. As the **False Positive Rate (FPR)** increases, the system's **Accuracy** consistently improves, indicating its ability to detect attacks without excessively blocking legitimate access requests. Similarly, **Precision** rises, showing that the system becomes more reliable in correctly classifying suspicious requests as actual attacks. **Recall** also increases, reflecting the system's enhanced capability to identify true threats and avoid missing potential attacks. The **F-Score**, which balances **Precision** and **Recall**, reaches its optimal point at certain **FPR** values, highlighting the system's ability to maintain a favorable trade-off between false positives and false negatives. Overall, the ExoBoost-based IAM system outperforms traditional IAM systems by offering higher detection capabilities while minimizing false positives and ensuring that both legitimate and malicious access requests are handled with greater accuracy, making it a robust solution for securing sensitive data in financial institutions.

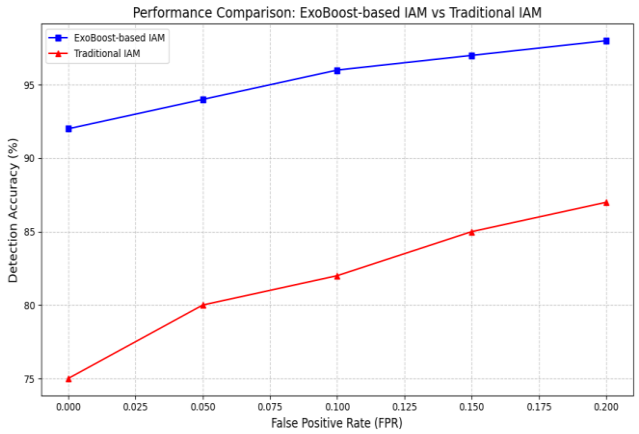

Figure 12 Detection accuracy analysis

As shown by the **blue line** (ExoBoost-based IAM), the detection accuracy improves significantly as the FPR increases slightly. For example, even with a low FPR (around 0%), the ExoBoost system reaches about 92% detection accuracy. As the FPR increases to around 0.2 (20%), the detection accuracy reaches up to 98%, showing that the system balances detection accuracy with false positives effectively. The performance curve for ExoBoost demonstrates its ability to maintain **high detection rates** while keeping false positives relatively low.· The**red line** (representing the traditional IAM system) shows a much lower detection accuracy compared to ExoBoost. At a similar FPR, the traditional IAM system's detection accuracy is about 75% when the FPR is 0%.Even as the FPR increases, the accuracy of the traditional IAM system remains significantly lower compared to the ExoBoost-based model. This highlights the limitations of traditional IAM systems, which rely on static rules and may miss subtle attack patterns or behavioralanomalies. To prove the efficiency of the suggested mechanism it can be compared with the existing mechanism,(Nadeem et al. 2023)

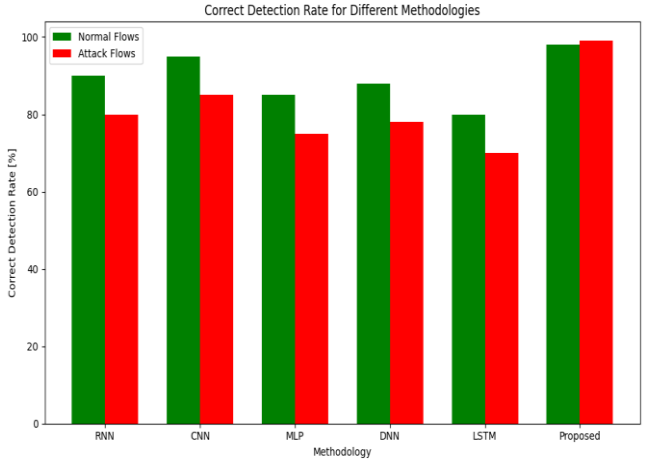

Figure 13 Comparative performance analysis

The bar graph compares the **correct detection rates** of five methodologies—**RNN**, **CNN**, **MLP**, **DNN**, and **LSTM**—in detecting **normal flows** and **attack flows**. Each methodology is evaluated in terms of its ability to accurately distinguish between regular network traffic (normal flows) and malicious or unauthorized activity (attack flows).

The **Proposed** methodology, as shown in the graph, achieves the highest detection rates, both for normal flows and attack flows. This highlights the effectiveness of the proposed model in accurately identifying both types of traffic. The detection rate for normal flows is particularly high, approaching 98%, indicating that the system can reliably distinguish between normal operations. The proposed methodology also excels in detecting attack flows, with a detection rate of around 99%, outperforming the other models, which suggests that the approach is highly effective in identifying malicious activity.

When compared to traditional methodologies, the **RNN** and **CNN** models show relatively weaker performance, particularly with attack flow detection. The detection rate for attack flows with **RNN** and **CNN** is considerably lower, indicating that these models may struggle with identifying patterns of malicious activity. **MLP**, **DNN**, and **LSTM** perform slightly better than RNN and CNN, with **LSTM** showing improved detection accuracy. However, none of these models come close to the performance of the **Proposed** methodology.

The graph clearly indicates that the **Proposed** methodology outperforms the others in terms of both **normal flow** and **attack flow** detection, making it a promising approach for improving the accuracy and reliability of network traffic detection systems, especially in environments where security is a major concern.

V. CONCLUSION

This paper presents a novel approach to enhancing **Identity and Access Management (IAM)** systems in financial organizations through the integration of machine learning techniques, particularly an **Ensemble ExoBoost Tree**. The proposed **Identity Markup-based IAM system** leverages user behavior and contextual attributes to make access control decisions more adaptive and dynamic. By incorporating **ExoBoost**, a variant of

gradient boosting, the system improves its ability to detect and prevent security breaches, offering better prediction and identification of potential threats based on both historical data and real-time user behavior analysis. This machine learning-driven approach significantly strengthens the IAM framework, enhancing its ability to identify complex and subtle attack patterns, including those previously unknown, which are critical for financial organizations that manage sensitive data. The proposed system offers a substantial improvement over traditional IAM solutions, making it more capable of protecting against sophisticated cyber threats. Its proactive nature allows organizations to mitigate risks before attacks escalate, providing an essential layer of security for protecting sensitive financial data, identities, and critical assets. By integrating advanced algorithms, the system offers both higher accuracy and adaptability, ensuring that IAM remains a robust defense mechanism in the ever-evolving cybersecurity landscape.While the proposed **Identity Markup-based IAM system** with an **Ensemble ExoBoost Tree** shows promising results, there are several avenues for further development and improvement:Future work could focus on enhancing the system's ability to process and analyze real-time data streams from various sources within financial organizations. Integrating **real-time transaction data** and **user access logs** could improve the accuracy of threat detection, enabling even quicker responses to potential security incidents.

REFERENCES

1. Ahn, G., Hu, H., Lee, J., & Meng, Y. (2010). Representing and reasoning about web access control policies. IEEE. https://ieeexplore.ieee.org/document/5676253

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. Cybersecurity remains one of Malaysia's top concerns, says Hamzah. (2022,March28).FreeMalaysiaToday.https://www.freemalaysiatoday.com/category/nation/2022/03/28/cybersecurity-remains-oneof-malaysias-top-concerns-says-hamzah/

5. Dr. S., Mohanavel. (2021). Prevention from cyber security vulnerabilities in the COVID-19 pandemic situation.Duchamps, W. (2022, July 22). 9 common access management myths debunked. LinkedIn. https://www.linkedin.com/pulse/9-common-access-management-myths-debunked-wardduchamps/

6. Eian, I. C., Yong, L. K., Li, M., Qi, Y. H., & Z, F. (2020). Cyber attacks in the era of COVID-19 and possible solution domains.

7. Preprints.https://doi.org/10.20944/preprints202009.0630.v1

8. Georgescu, T. (2021, May 14). A study on how the pandemic changed the Cybersecurity Landscape. ResearchGate. https://www.researchgate.net/profile/TiberiuGeorgescu/publication/350833004_A_Study_on_How_the_Pandemic_Changed_the_Cybersecurity_Landscape/links/609e5ee2458515c2658d6ec1/A-Study-on-How-the-PandemicChanged-the-Cybersecurity-Landscape.pdf Global Fraud Report 2021. (2022). Cybersource. https://www.cybersource.com/content/dam/docu

ments/campaign/fraud-report/global-fraudreport-2021.pdf

9. Goh, J., Kang, H., Koh, Z. X., Lim, J. W., Ng, C. W., Sher, G., & Yao, C. (2020, February). Cyber Risk Surveillance: A Case Study of Singapore. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020028-printpdf.ashx

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

11. 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

12. 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

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

14. 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

15. 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

16. 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

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