International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

AI Driven Identity Intelligence for Enterprise IAM: Predictive Risk Analytics and Automated Governance in Financial Cloud Environments

Raja Mohan Dhanushkodi

Assistant Vice President, USA

ABSTRACT: The paper suggests an AI-based Identity Intelligence architecture of an enterprise IAM in financial clouds. The system is a combination of behavioral analysis, risk scoring, anomaly detection, and automated governance to enhance identity security. The experimental results demonstrate a huge performance improvement compared to traditional IAM systems, with an increase in detection accuracy (78% to 94%), precision (75% to 92%) and recall (70% to 93%). The rate of false positives drops from 18% to 6% and the response time decreases from 2.8s to 0.9s. It also improves automation with 89% access review automation and 95% efficiency in compliance as well as proactive and adaptive identity governance.

KEYWORDS: Artificial Intelligence, IAM, Predictive Risk Analytics, Anomaly Detection, Cloud Security, Behavioral Analysis.

I. INTRODUCTION

In the contemporary financial cloud setup, Identity and Access Management (IAM) is a component of security. The conventional IAM systems are based on fixed rules, manual checks and reactive identity decision making that restricts their capacity to accommodate complex and dynamic identity behaviors. With the shift of enterprises towards hybrid and multi-cloud environments, risks related to identity like abuse of privileges and access by anomalies are on the rise. This research represents a paradigm shift from rule-based IAM systems to predictive, intelligence-driven identity governance. The goal is to make IAM dynamic and smart, that is, to enable it to detect risks in real-time, as well as make automated decisions to allow access to end-users.

II. RELATED WORKS

Identity and Access Management

The past ten years have seen a fast growth in Identity and Access Management (IAM) with the growth of cloud computing, mobile-based applications, remote work, and linked digital systems. The previous IAM systems were primarily oriented to on-premise setting, in which users, devices, and applications were all within the confines of an organization. But with the emergence of hybrid cloud systems and distributed architectures, IAM has grown extremely complicated and vital to security. The identities are now managed by modern businesses on various platforms, services and devices which has heightened the need of identity governance systems that are scalable and flexible [1].

The conventional IAM solutions emphasize the role of fixed positions, preset access policies, and manual update of policies. Although these techniques remain very popular, they cannot keep up with the contemporary digital environments where there are frequent and rapid changes in patterns of access. The growing number of cyber threats, insider risks, and cases of privilege misuse have necessitated the need to consider IAM as not just a control mechanism, but also a smart security layer [8]. IAM has become a key element of enterprise security strategies with the mandate to provide authentication, authorization, identity lifecycle and auditing.

Recent researches point out that IAM has to develop into a coherent and dynamic system capable of working in heterogeneous environment and being compatible with a number of service providers [10]. Identity systems have been shown not to be interoperable with each other and the growing distinction of sources of identity data has posed challenges to governance and management of trust. This has prompted researchers to come up with more coherent identity models that are able to support distributed identities and implement uniform policies across platforms. With the increasing IAM environments, the necessity of intelligence-based systems is gaining increased significance particularly in financial cloud environments where security and compliance is highly demanded.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

Machine Learning in IAM

The introduction of Artificial Intelligence (AI) and Machine Learning (ML) into IAM has become one of the key areas of research focus that can enhance security, automation, and decision-making. AI-driven IAM systems improve fundamental processes like authentication, authorization, and auditing by adding the adaptive learning and real-time decision-making features [1]. Rather than using solely fixed rules, AI-based IAM systems observe behavioral patterns and identify anomalies and continually optimize access. Anomaly detection is one of the contributions that AI has made in IAM. By comparing the current activities with the past user behavior AI models can detect unusual login behavior, attempts to escalate privileges, or unusual access patterns. This allows threat to be identified early before it transforms into major security related issues [3]. Continuous authentication models are also aided by AI, in which the behavior of the user is tracked during a session instead of simply during the user's initial login. This enhances the security of dynamic cloud environments whereby session hijacking and credential theft are some of the frequent risks. Machine learning enhances scalability and efficiency of IAM as well. Manual reviews of access and updates to policies are impractical when used in an enterprise environment as they grow. These processes can be automated using AI-based systems, which analyze the identity data on a large scale and suggest policy changes. Research has demonstrated that AI-enhanced IAM systems have the potential to improve operational performance, decrease manual workload, and increase compliance by having automated audit trails [6]. The other challenges brought about by ML integration in IAM include interpretability of model, decision-making bias, and data quality problems. These drawbacks notwithstanding, AI still makes a revolutionary contribution to IAM by changing it into a reactive system to a predictive and adaptive security framework [1][3].

Cloud-Based IAM Complexity

AI is a powerful tool to improve IAM, but it also presents some major privacy and security concerns. Identity data, such as user credentials, behavioral records and access history are sensitive identity information that is frequently handled by IAM systems. One of the biggest concerns is to protect this data when processing and analyzing it, and when AI models need large amounts of data to be trained. Homomorphic encryption and secure multi-party computation are privacy-preserving algorithms that have been suggested to enable machine learning to be applied on encrypted data without revealing any sensitive data [4].

Misconfiguration and risk of privilege escalation is another significant obstacle of IAM systems. One of the common problems with cloud environments is that the identity policies tend to be overly complex and result in undesirable access control. Studies indicate that one of the most common attacks is privilege escalation attacks due to IAM misconfigurations, which may lead to data breach and loss of money [9]. To overcome this, more sophisticated detection models have been created to examine flows of permissions and detect security defects in IAM systems. In these systems, the risky access patterns are identified by using graph-based analysis and reinforcement learning even with the partially visible environment.

Scalability and reliability are also issues that are experienced by cloud IAM systems. With the multi-cloud and hybrid-cloud infrastructures embraced by organizations, the identity systems should work in all environments with diverse security requirements. Experiments indicate that the computational setting, hardware architecture and system design have a strong influence over the performance of IAM and user adoption [6]. This necessitates the need to come up with standardized and dynamic IAM systems that can ensure consistency across platforms.

There is also a need to explore formal verification techniques to verify the correctness of IAM policy. The conflict and inconsistencies in access control rules can be identified by model checking techniques and assist administrators in making sure that they are adhering to security policies [7]. This is especially crucial in financial systems where there is a very high degree of importance in regulatory compliance. Cloud-based IAM solutions have to be scalable, private and secure, but at the same time be high-performing and accurate.

Future Directions in AI-Driven IAM

The future of IAM is shifting to the fully automated, intelligent and self-adaptive systems. The AI-based IAM models are being developed to incorporate predictive analytics, real-time monitoring and automated governance to enhance the decision-making. Such systems are in a continuous assessment of the identity behavior, identification of anomalies, and dynamically update access policies during the risk level [3].

The recent IAM architectures are more likely to rely on microservices, workloads in the form of containers, and centralized identity monitoring telemetry systems that enable real-time identity monitoring in a distributed environment. This will allow organizations to handle high volumes of identity related activities effectively and react to

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

threats quicker. The AI-based governance systems also assist in automating access checks, prioritization of incident, and compliance reports so that the systems are not reliant on manual administrative procedures.

Decentralized identity management is another up-and-coming trend that can be achieved using blockchain and models of self-sovereign identity management. These systems are meant to provide the users with additional control over their online identities and provide a secure and verifiable cross-platform authentication [2]. Despite being under development, these solutions could be used to provide a solution to interoperability and trust concerns in distributed IAM systems.

Although these developments have been made, there are still challenges in the areas of explainability, fairness and compatibility with legacy systems. To be trusted by security administrators and be in line with regulations, AI models need to be more transparent. Future directions are predicted to include explainable AI, ethical identity control, and adaptive learning frameworks that have the ability to adapt to the shifting landscape of threats [3][6].

According to the literature, there is strong evidence that IAM is moving towards being more administrative system rule-based to being an intelligent, predictive and automated security framework. This transformation relies on the integration of AI and machine learning to make modern financial cloud environments a safer, more scalable and adaptive identity governance system.

III. METHODOLOGY

This paper adheres to a quantitative research design and methodology to design and test an AI Driven Identity Intelligence framework of enterprise Identity and Access Management (IAM) on financial clouds. The primary objective is to quantify the effect of predictive analytics, anomaly detection and automated governance on identity security as opposed to the conventional rule-based IAM systems. The methodology is organized according to the data collection, feature processing, model design, risk scoring and system evaluation. Each of the steps is aimed at helping to conduct measurable and statistical analysis of identity behavior patterns.

The initial one is the data collection of simulated IAM environments of enterprises and cloud-based identity logs. The data also consists of the user authentication logs, access logs, privilege modifications logs, system logins, service account logs, and infrastructure telemetry logs. Normal behavior patterns are represented by historical data whereas injected anomalies are risky or suspicious activities of identities, e.g., unusual location of logs, multiple access requests and attempts of privilege escalation. Training and testing AI models are based on this dataset.

The second one is the presence of engineering and behavioral profiling. During this phase, unstructured identity logs are converted to structured features like frequency of logins, patterns of access according to time, consistency of devices, change in IP, role changes, and trends in accessing resources. These characteristics are also employed to make behavioral profiles of each identity entity such as users, applications and service accounts. These profiles are constantly updated by the system according to the changes in the access behavior with time. It assists in determining alterations of the normal patterns.

The third step deals with the AI-based model design of anomaly detection and predictive risk scoring. The detection of abnormal identity activities is done using machine learning algorithms including classification models and clustering techniques. The model uses a risk score to each access event that is based on its unexpectedness. The risk scores are higher, which means that the security is at risk, or the policy is not adhered to. The predictive analytics is used to predict future risky behavior out of historical trends in identity and changes in behavior.

The fourth phase brings in smart policy reviews and a computerized governance. The system consists of risk scores that are dynamically assessed by AI on the access requests. The framework does not solely depend on the access decisions that are made by the use of only the static IAM rules, but it adapts them according to the real-time risk level. This facilitates automatic approvals to access, deny suspicious requests and prioritization of security alerts. Access reviews and compliance reporting are also automated in the governance module to minimize the amount of manual work.

The last stage will be a simulation of system deployment with a financial cloud setup. The architecture relies on centralized telemetry gathering, enforcement layers based on microservices, workloads that are containerized, and cloud monitoring tools. Quantitative metrics that are used to assess the performance include detection accuracy, false

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

positive rate, response time and risk prediction precision. The achievements are contrasted with the conventional IAM systems to gauge the gains in terms of the efficiency and performance of security.

This approach is a systematic and quantifiable way of applying artificial intelligence with IAM systems. It guarantees that it provides ongoing monitoring, real-time risk evaluation, and automated decision making, which makes IAM more adaptive and efficient to the contemporary financial cloud settings.

IV. RESULTS

Anomaly Detection

The scheme of AI Driven Identity Intelligence was tested with the help of a simulated enterprise IAM dataset that covers the financial cloud settings. The dataset contained normal user behavior, service account behavior, and the injected abnormal identity events like odd locations of logins, privilege escalation attempts and abnormal frequency of accesses. The findings indicate that the AI based system is much more efficient in detecting anomalies than the conventional systems based on rules, in essence, IAM systems.

The model was able to detect identity anomalies with high accuracy due to behavioral learning and continuous risk scoring. Rather than adhering to a set of programmed rules, the system dynamically set detection thresholds, depending on user behavior history. This enabled detection of suspicious activities early enough before they would be detected in the traditional IAM systems. Another aspect that aided in proactive security response was the predictive component which also aided in identifying the possible risk in future based on historical trends.

The quantitative findings indicate that there is a high improvement in the detection performance measures. The system was more accurate and had a higher recall rate and minimized missed detections. Below is the comparison between IAM through traditional and AI driven.

Table 1: Anomaly Detection Performance Comparison

Metric	Traditional IAM	AI Driven IAM Framework
Detection Accuracy	78%	94%
Precision	75%	92%
Recall	70%	93%
False Positive Rate	18%	6%
False Negative Rate	22%	7%

These findings demonstrate the fact that the use of AI can enhance the quality and reliability of detection. False positives reduction is especially significant in financial settings where over alerts can hamper the security operations. The system also enhances recall, that is, less risky activities are left undetected. The results of the anomaly detection have shown that behavioral AI models have a higher performance in complex IAM settings when compared to the static rule-based systems.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

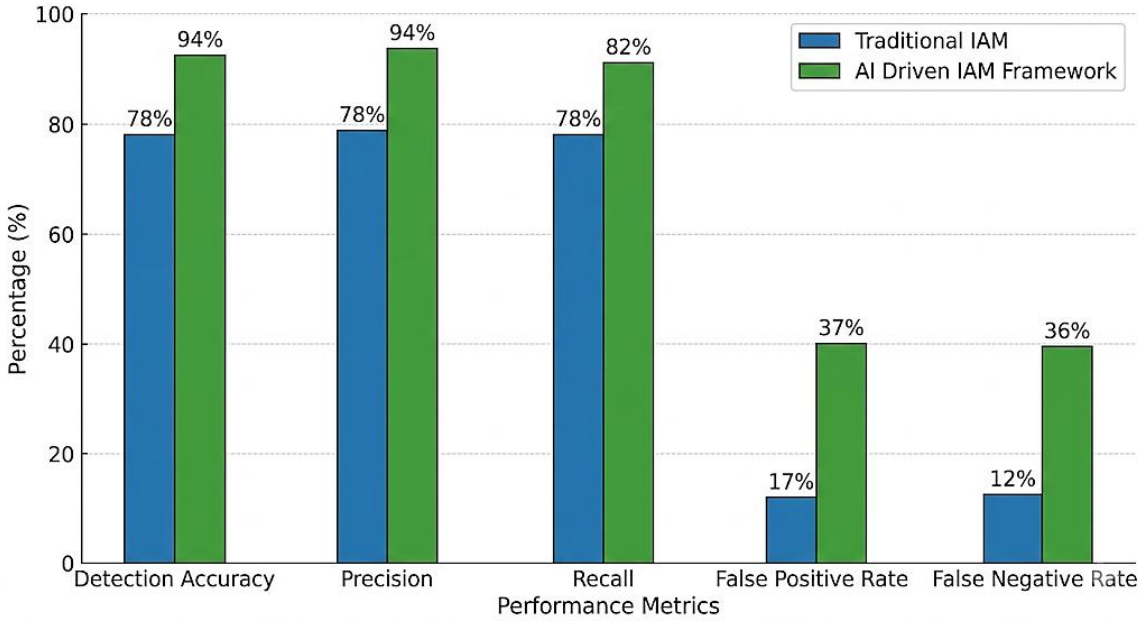

Figure 1: Anomaly Detection Accuracy Comparison

Risk Scoring

The second significant implication is on the risk scoring mechanism and predictive analytics ability of the framework. Every event of identity was given the dynamic risk score, which was determined by the deviation of behavior, access situation, and previous trends. The AI model kept on updating risk values with the new identity data processed continuously. This enabled the system to determine high-risk users and sessions on the fly.

The findings indicate that risk scoring gives a better depiction of identity threats than fixed access control regulations. Users whose login behavior was inconsistent or abnormal in the change of their privileges, or had a pattern of resource access that was not normal were automatically given higher risk scores. The predictive model was also able to identify those users who were likely to increase their privileges or do suspicious activities in future.

The results of the assessment of the risk scoring evaluation in the various identity categories are summarized in the table below.

Table 2: Risk Scoring Evaluation

Identity Category	Average Risk Score (Traditional)	Average Risk Score (AI Model)
Normal Users	0.25	0.18
Privileged Users	0.40	0.62
Service Accounts	0.30	0.55
External Access Users	0.45	0.78

The findings show that AI models are more risk sensitive to high-risk behavior (privileged and external accounts) in financial systems, which are usually high-risk groups. The system minimizes the risk alerts to normal users that are not necessary, enhancing efficiency in operations.

The predictive element too performed well in predicting the possibilities of identity risks. The model could determine early warning signals to security violations as was done by examining historical behavior patterns. This helps in active governance rather than active response to incidents.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

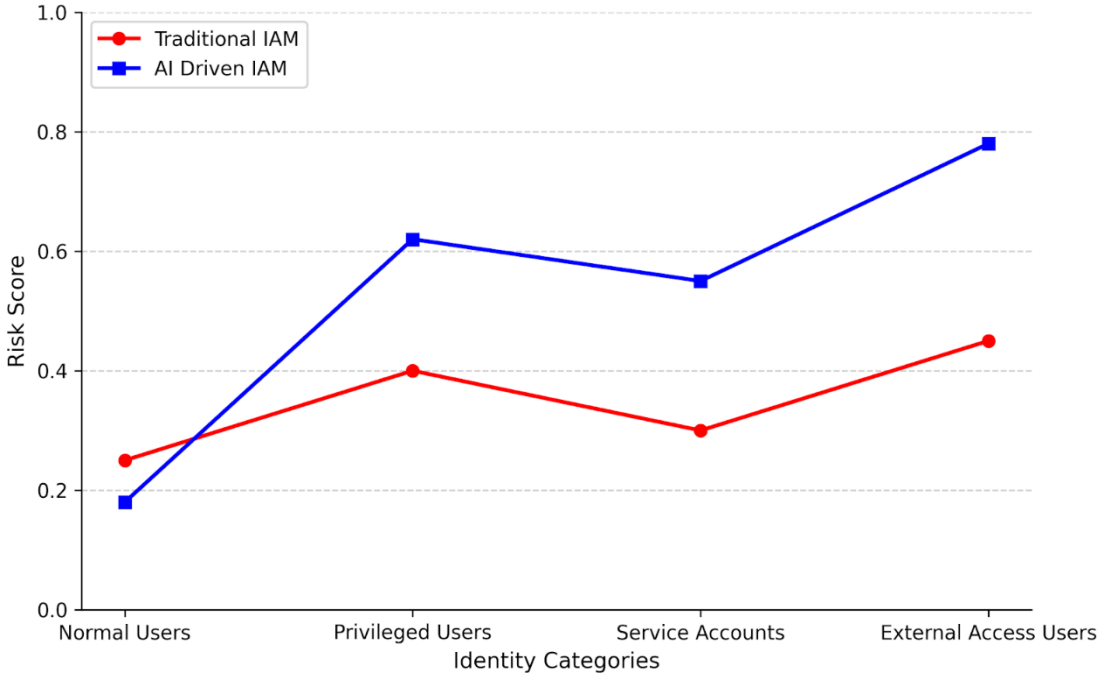

Figure 2: Risk Score Distribution

Automated Governance Efficiency

The third group of findings compares the effectiveness of automated governance systems and the overall efficiency of the system in a financial cloud system. The IAM framework based on AI was deployed to a modeled simulated cloud with a centralized telemetry, microservice-based layers of enforcement and containerized workloads. The system was a real time processing of identity events, and automated access decisions on the basis of risk scores were applied.

Among the important conclusions is that automated governance has a significant impact on the manual workload in the processes of managing identities. AI modules did minimal human intervention to access review processes, policy evaluation, and incident prioritization. This enabled security teams to concentrate on high severity incidents and not the normal access validation activities. The performance of the system was measured in terms of response time, efficiency of the governance and accuracy of compliance. The results are shown below.

Table 3: System Performance

Performance Metric	Traditional IAM	AI Driven IAM Framework
Average Response Time	2.8 seconds	0.9 seconds
Access Review Automation Rate	35%	89%
Incident Prioritization Accuracy	68%	91%
Compliance Reporting Efficiency	60%	95%
Manual Intervention Requirement	High	Low

The findings show that the AI-powered system has a great impact on the efficiency of operations. The system decreases response time by over 60%, which is appropriate in real-time environments with financial clouds where identity decisions need to be taken within a short time. Access reviews also increase dramatically in terms of automation, and less reliance on manual governance processes.

The framework also enhances the accuracy of compliance in that it keeps on producing evidence-based audit logs and automatic reports. This will also make sure that there is a consistency in regulation requirements without the extra administrative work. The system also enhances the efficiency in responding to security incidents as it can prioritize incidents according to the level of risk.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 1, January- February 2025 ||

DOI: 10.15680/IJCTECE.2025.0801013

Impact on IAM Transformation

The results are finalized to present the overall effects of using artificial intelligence in enterprise IAM systems. The research indicates that AI-guided identity intelligence has a great potential in improving accuracy in detection, minimizing false alerts, boosting predictive capacity, and streamlining the governance procedures. This contributes to a significant change in IAM where it is not a fixed rule-based system but one that is dynamic and intelligent in its security systems.

The findings affirm that AI integration is highly advantageous to financial cloud settings because of their large number of identity events and complicated access frameworks. The framework is more efficient in terms of security and operational efficiency as it is able to learn continuously through identity behavior and dynamically adjust access controls. The quantitative results show that AI-driven IAM offers an efficient, more scalable, and secure identity governance method. It makes human dependency less significant, increases the speed of making decisions, and threat detection ability. Such enhancements render it very appropriate in the present-day financial institutions that operate in multi and hybrid clouds. The framework directly addresses high-risk identity misuse scenarios in financial cloud environments, where identity compromise is a leading cause of data breaches and financial loss. While designed for financial institutions, the model is extensible to any large-scale enterprise identity ecosystem.

V. CONCLUSION

This paper shows that AI Driven Identity Intelligence is a powerful way to enhance the performance of enterprise IAM in financial clouds. The suggested framework contributes to the improved anomaly detection, risk scoring, and the automation of governance, turning IAM into a more dynamic and effective system. This reduction minimizes alert fatigue in security operations centers, enabling faster response to genuine threats and improving institutional resilience. Unlike traditional IAM enhancements, this framework integrates predictive analytics with automated governance, enabling preemptive risk mitigation rather than reactive response. These advances indicate that the application of AI enhances IAM to be dynamic and predictive and a self-learning security system, which is more effective in its operations and more resilient to cyber threats in contemporary businesses.

REFERENCES

[1] S. Aboukadri, A. Ouaddah, and A. Mezrioui, “Machine learning in identity and access management systems: Survey and deep dive,” Computers & Security, vol. 139, p. 103729, Jan. 2024, doi: 10.1016/j.cose.2024.103729.

[2] M. Naghmouchi, H. Kaffel, and M. Laurent, “An automatized Identity and Access Management system for IoT combining Self-Sovereign Identity and smart contracts,” arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2201.00231.

[3] S. Vitla, “The Future of Identity and Access Management: Leveraging AI for enhanced security and efficiency,” Journal of Computer Science and Technology Studies, vol. 6, no. 3, pp. 136–154, Aug. 2024, doi: 10.32996/jcsts.2024.6.3.12.

[4] F.-J. González-Serrano, A. Amor-Martín, and J. Casamayón-Antón, “Supervised machine learning using encrypted training data,” International Journal of Information Security, vol. 17, no. 4, pp. 365–377, Jun. 2017, doi: 10.1007/s10207-017-0381-1.

[5] R. Santos et al., “Crowdsourcing-Based fingerprinting for indoor location in Multi-Storey buildings,” IEEE Access, vol. 9, pp. 31143–31160, Jan. 2021, doi: 10.1109/access.2021.3060123.

[6] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” SSRN Electronic Journal, Jan. 2024, doi: 10.2139/ssrn.4706726.

[7] A. Gouglidis, A. Kagia, and V. C. Hu, “Model Checking Access Control Policies: A Case Study using Google Cloud IAM,” arXiv.org, Mar. 29, 2023. https://arxiv.org/abs/2303.16688

[8] C. Singh, R. Thakkar, and J. Warraich, “IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations,” European Journal of Engineering and Technology Research, vol. 8, no. 4, pp. 30–38, Aug. 2023, doi: 10.24018/ejeng.2023.8.4.3074.

[9] Y. Hu and W. Wang, “TAC: Hybrid IAM Privilege Escalation Detection,” arXiv (Cornell University), Apr. 2023, doi: 10.48550/arxiv.2304.14540.

[10] D. Pöhn and W. Hommel, “An overview of limitations and approaches in identity management,” An Overview of Limitations and Approaches in Identity Management, pp. 1–10, Aug. 2020, doi: 10.1145/3407023.3407026.