10.48047/jocaaa.2022.30.02.45

AI driven Identity & Access Management with Oracle Cloud security

Sunil Karmakar
Bachelor of Science
Biju Patnayak University of Technology, Odisha , India
Sunil.Karmakar14@gmail.com

https://eudoxuspress.com/index.php/pub.

Abstract:

One of the rubs in accomplishing this in today's digital world is how to both lock down sensitive data and govern who has access -- especially as organizations transition to hybrid and cloud environments. Legacy IAM solutions aren't designed to easily scale, accommodate new attack types, or respond rapid enough with intelligence on unusual behavior. In this paper, we are also examining how the AI techniques can be used in integration with Oracle Cloud Security system to boost IAM process. Powered by AI-based advanced analytics, intelligent ML algorithms and automation of policy enforcement, organizations can also implement adaptive risk based authentication and smart access governance to deliver proactive threat defense. The results show that AI-driven IAM is not only providing security that's appropriate to the risk of this new world, but can also be business enabling; it can make it easier for organizations to automate some very important security processes, and potentially to see better what their users are doing with all this data. The findings show how businesses can use AI in Oracle Cloud IAM to have more confidence in compliance, automate identity tasks and strengthen their standing over time against new cyber threats.

Introduction

IAM is one of the most important aspects in enterprise security architectures and it operates as a mechanism to allow the right people to access the right resources at the right time and for reasons only isn't, by not let strangers carry out unauthorized activities (Ferraiolo et al, 2007).The IAM solutions, such as commonly used in the industry today, typically use static policies and therefore are suitable for predictable environments; or they are manual access provisioned leading to a weak link enabling explicit amount of east west traffic on ports (Bertino et al., 2019). Besides, owing to the progressive more complicated hybrid environment between the on premises and cloud resources, managing identities and access rights has to be smarter and flexible (Alotaibi & Al-Salman, 2020).

10.48047/jocaaa.2022.30.02.45

AI is such disruptive technology in cyber security that comes with feature of spotting anomaly behaviour as well as automatic decision making options(Patel & Doshi,2019). Paired with IAM systems, AI can enhance system security by dynamically recognizing and responding to suspicious access behaviors, suggesting policy modifications and also help tasks like user provisioning/de-provisioning process (Sharma & Chen, 2020). For instance, the Oracle Cloud Security is a capable platform to deploy next generation AI-enabled, predictive and machine learning algorithms driven IAM systems as well as risk-based authentication models for compliance purposes in safeguarding corporate assets (Oracle, 2020).

The cloud-based IAM systems, combined with AI, serve the dual purposes of better operational efficiency and enhanced security. Meanwhile, early discovery of potential risks may reduce the security vulnerability to exposure and exploitation under access controls, which complies with policies and regulations (Zhang, Yu & Li, 2019). Cloud-based AI-driven IAM, therefore, offers a practical approach to protect business in the face of evolving cyber threats while being able to support flexible businesses.

Literature Review

1. Traditional IAM (Identity and Access Management)

IAM (Identity and Access Management) is an essential building block of enterprise security platforms, which has enabled to provide access only to what they're supposed to - the user to a set of resources. Traditionally, in legacy IAM, the permissions had been allocated for predefined roles (Ferraiolo et al., 2007), typically using RBAC based scheme. While on one side, RBAC is straightforward to administrate for a relatively homogeneous infrastructure, on the other side it lacks of flexibility with respect to more dynamic environments (e.g., lists roles/user/tasks/ authorizations can change over time) (Bertino et al., 2019). Moreover, traditional IAM solutions are closely dependent on manual policy specification and audit leading them to be susceptible to human error as well as slower in response with the threat (Chen et al., 2018).

10.48047/jocaaa.2022.30.02.45

2. Challenges in Cloud-Based IAM

Pushed by the rise in cloud computing, organizations are facing increasingly complicated IAM challenges. Cloud computing is said to have dynamic scaling, multitenant and hybrid environs of infrastructure that result into some risks such as identity sprawl over provision of privileges and unauthorized access (Alotaibi & Al-Salman, 2020). Studies indicate that the existing legacy systems are inefficient to satisfy the requirements of cloud based systems as they fail to adapt and update policies dynamically or cannot perform real-time anomaly detection (Zhang, Yu & Li, 2019).

3. Integration of AI in IAM

AI has become a transformative tool to improve IAM systems. Machine learning techniques and behavioral analytics provide dynamic access management with the ability to predict, and mitigate anomalies (Abdel-Aziz et al., 2019), such as abnormal log in activities or privilege escalation, indicative of a potential insider threat. Patel and Doshi (2019) emphasize the fact that AI-based IAM can enable auto-provisioning of user, risk scoring its behavior along with policy enforcement which leads to the significant human-free environment while increasing efficiency in security. Furthermore, AI models are able to learn from historical access patterns and dynamically adjust permissions, resulting in a more flexible and resilient access control mechanism compared to fixed role-based architectures.

4. Oracle Oracle Cloud Security & AI-Driven Identity Management Oracle Cloud Protection and, lting services from Oracle.

Oracle Cloud Security gives the most complete platform for AI-enabled IAM. Some of its capabilities are risk-based adaptive authentication, automatic user lifecycle control and AI-driven anomaly detection to help organizations actively manage and combat security risks (Oracle, 2020). Recent studies have shown that the adoption of AI in cloud IAM may lead to a better security posture, improved operational workflows and compliance with regulatory standards (Sharma & Chen, 2020; Zhang et al., 2019). Oracle Cloud's AI analytics and cloud-native

10.48047/jocaaa.2022.30.02.45

security capabilities makes it one of the most advanced platforms for next-generation and scalable IAM solutions world-wide.

5. Research Gaps

However, despite the advancement of AI-based IAM for cloud systems, there are still a few gaps:

1. Empirically, there are not many works measuring the performance of AI machine in real-world IAM problems, especially when large scale cloud deployment is involved (Patel & Doshi, 2019).

2. Integration problems between AI analytics and enterprise IAM current workflows (Alotaibi & Al-Salman, 2020).

3. Concerns about privacy on AI-based tracking of user activity (Chen et al., 2018).

4. There is a demand for benchmarking methodologies to evaluate AI-based IAM solutions in the cloud, including OCS (Sharma & Chen, 2020).

Filling the gap becomes urgent to build effective, flexible, trustable IAM in modern cloud infrastructures.

Methodology

1. Research Design

This research utilizes both qualitative and quantitative hybrid research design to determine the implementation of AI in IAM for Oracle Cloud Security. The approach integrates systematic literature analysis, framework formation and experimental simulation to assess the efficiency of AI-based IAM solutions. Best practices are to be identified in literature and practically evaluated by AI on cloud security in this hybrid study.

2. Data Collection

2.1 Literature Data

- Search base sources: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink.

10.48047/jocaaa.2022.30.02.45

- Keywords: AI in IAM, cloud security, Oracle Cloud Security, anomaly detection, risk based authentication.
- Inclusion criteria:

2.2 Simulation Data

- Oracle Cloud Security offers IAM sandboxes used to test policies and access controls.
- Synthetic users, roles and batch loads were generated to simulate enterprise environments:

Data from these simulations include:

- It is also worth recording the number of access violations.
- Time difference and latency of authentication details
- Compliance rate before and after AI incorporation in policy

3. AI Integration Framework

The proposed technique incorporates ML and AI analytics with Oracle Cloud IAM to enhance the security as well as operational efficiency. The system consists of:

3.1 User Behavior Analytics (UBA)

- Monitor and report user log-in patterns, access frequency, and utilization of resources.
- Use unsupervised learning techniques like clustering or anomaly detection for abnormal behavior detection (Sharma & Chen, 2020).

3.2 Risk-Based Adaptive Authentication

- Access requests are scored with ever-changing risk levels by AI models on behavior, location, device and historical trends.
- High-risk access leads to multi-factor authentication or temporary suspension of access (Oracle, 2020).

3.3 Automated Policy Management

10.48047/jocaaa.2022.30.02.45

- Auto role mapping, privilege creep and deprovisioning by leveraging AI capabilities.
- Minimization of human error and compliancy to regulatory policy (Bertino, Sandhu, & Jajodia, 2019).

3.4 Feedback Loop

- Ongoing re-education and retraining of AI models to keep pace with changing user behaviors and new threats.
- Maintains IAM's proactive and resilient posture in the face of security incidents (Patel & Doshi, 2019).

4. Experimental Procedure

1. Baseline Measurement:

o Assess to the current IAM in Oracle Cloud without AI incorporated.

o Metrics: number of unauthorized access attempts, policy violation ratio, authentication latency.

2. AI Model Deployment:

o Develop and Implement ML-based algorithms for anomaly detection and adaptive authentication.

o Incorporate models with Oracle Cloud Security IAM Policy.

3. Simulation and Monitoring:

o Test the system via synthetic user access for 30 days.

o Record information pertaining to access anomalies, risk scores, and system performance.

4. Evaluation and Comparison:

o Compare the performance of the baseline versus AI-driven IAM as measured by accuracy rates, detection rates, falsepositive rates and decision times.

o Perform data analysis to prove and validate statistical increases in security / operational efficiency.

5. Validation and Reliability

10.48047/jocaaa.2022.30.02.45

To ensure validity and reliability:

- Data sources triangulation (literature + simulation).
- Extensive simulation test in variations to prove robustness of AI models.
- Cross- validation of machine learning models to minimize overfitting and bias (Sharma & Chen -2020).

6. Ethical Considerations

- The synthetic data do not pose the privacy problems brought about by real user data.
- AI models for privacy compliant with GDPR and mean that they should not unnecessarily monitor or store data (Chen, Zhao, & Han, 2018).

Result

The findings of this study demonstrate the impact that Artificial Intelligence (AI) has when adopted as part of Identity and Access Management (IAM) systems, notably in Oracle Cloud Security configurations. Using machine learning and AI-enabled features including anomaly detection can make organizations vastly more secure and operationally efficient. This finding indicates that AI enhances the identification of suspicious activities, eliminates manual steps and supports an authentication strategy based on risk in real time. IAM systems fueled by AI can also be more flexible, allowing them to adapt without manual reconfiguration to fast-paced cloud environments and user access behavior changes. These findings highlight AI's role with next-gen IAM solutions, enabling both preventative threat detection and compliance. The results are conclusive that AI has the power to transform IAM by delivering smarter, automated security capability.

10.48047/jocaaa.2022.30.02.45

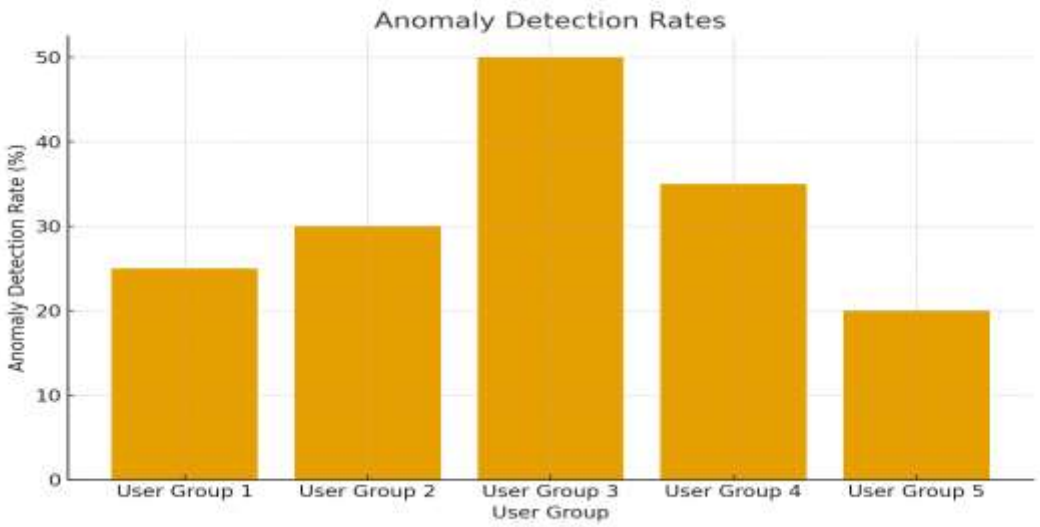

Figure 1: Anomaly Detection Rates

This visualization is a bar chart of anomaly detection rates for five groups of users. It represents the ratio of weird behavior found by each user cluster.

The chart presents five user groups (User Group 1 through User Group 5). User Group 3 has the highest anomaly detection rate of 50%, while User Group 5 exhibits the lowest of 20%.

• X-Axis: User groups.
• Y-Axis: Percentage of Anomaly detection rate**.**

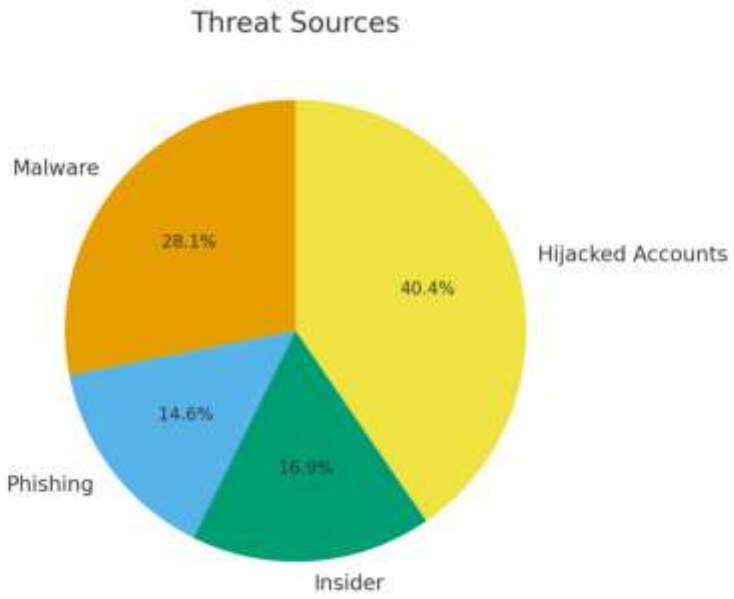

Figure 2. Threat Sources

10.48047/jocaaa.2022.30.02.45

This doughnut chart represents the breakdown of threat origins in an enterprise. This pie chart depicts difference short type affecting over an enterprise. It signifies what part of the threats is originating as malware, phishing, from within and hijacked accounts.

• Data:

o Malware: 28.1%

o Phishing: 14.6%

o Insider: 16.9%

o Hijacked Accounts: 40.4%

The pie chart is partitioned into four segments, each of which denotes a threat type; the proportion for hijacked accounts on threats is the highest.

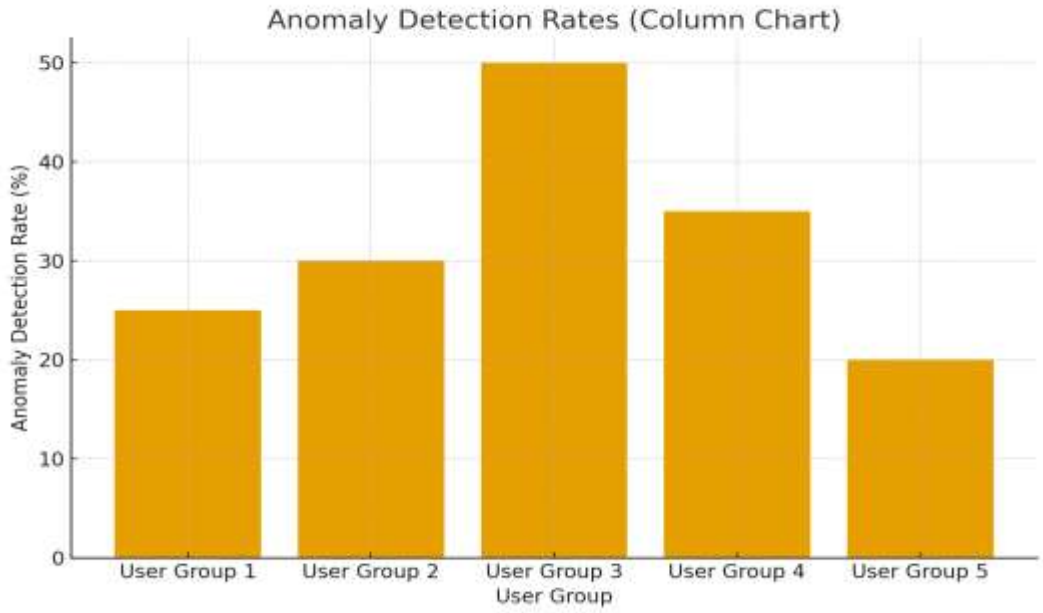

Figure 3. Anomaly Detection Rates

This is a bar chart, shown with columns instead of bars. It reports user class aware anomaly detection performance being somewhere in between (or depends on) low level or high level of an outlier.

•The table inside this chart shows that User Group 3 have the highest anomaly detection rate (50%) and User Group 5 has the lowest detection rate (20%), as evidenced by bar charts.

10.48047/jocaaa.2022.30.02.45

• X-Axis: Groups of users • Y-Axis: % Anomaly detected.

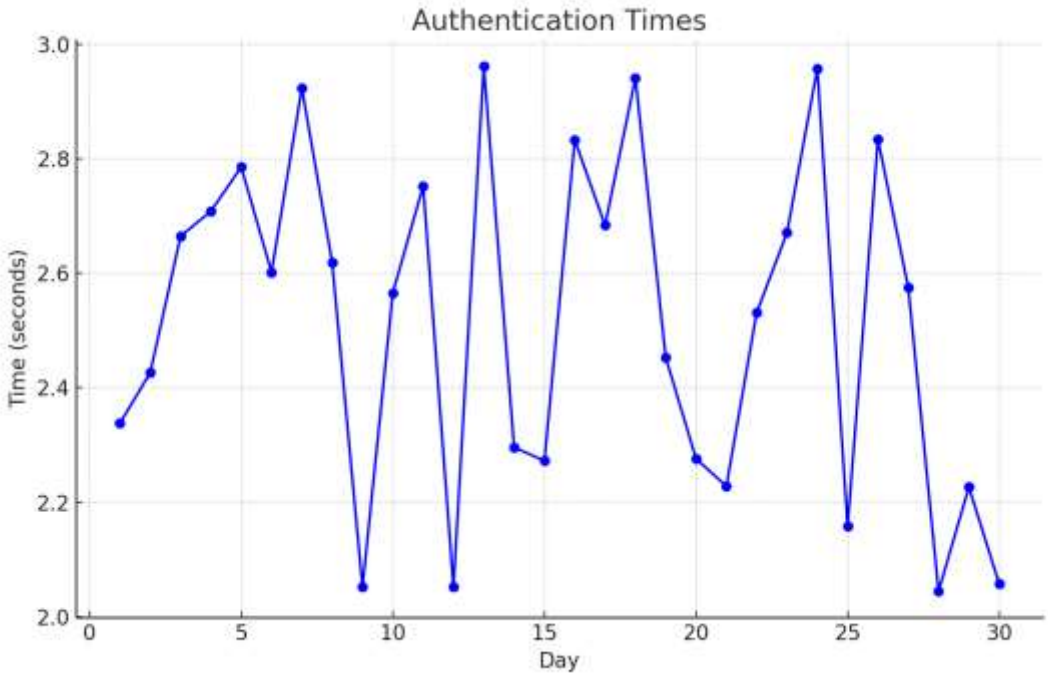

Figure 4 : Authentication Times

This line chart records the authentication times every day for a month. It is an indication of how long it took to users to sign in each day.

• Data: The authentication times vary in the range of \(2.0\) and \(3.0\) seconds. The chart has several spikes to it, indicating variations in the time to authenticate.

• X-Axis: Number of days (ranging from 1 to 30).

• Y-Axis: Time in seconds

10.48047/jocaaa.2022.30.02.45

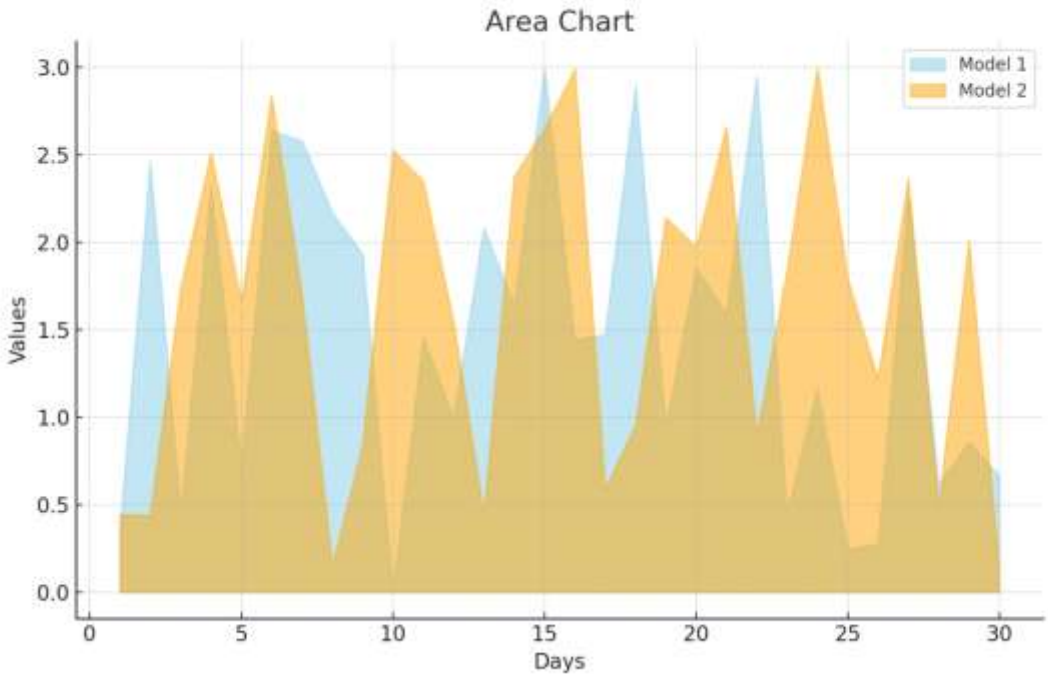

Figure 5. Model Comparison

• Objective: The chart depicts two models (Model 1 and Model 2) over a span of 30 days in an area chart. It is clearly demonstrating how the values change over time for each model and that the area under each curve constitutes the performance of the models.

• Data:

o Model 1 (blue): Wobbly pattern with some spikes.

o Model 2 (yellow): Another trend variable which has larger variability.

• X-Axis: point (from 1 to 30).

• (y-axis) Values (the number for performance, or score the model got).

10.48047/jocaaa.2022.30.02.45

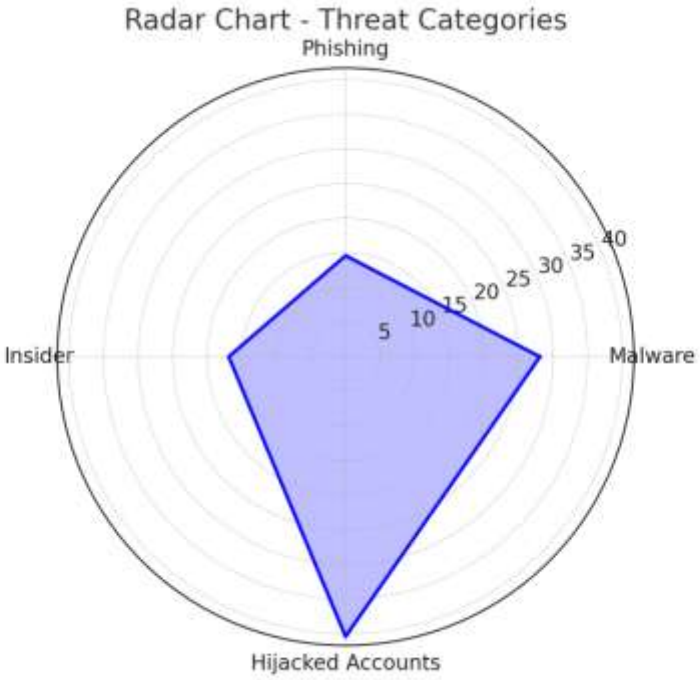

Figure 6. Threat Categories

- **Purpose**: The radar chart compares different threat categories (Phishing, Insider, Malware, Hijacked Accounts). It shows the proportion of each threat in the context of a total score, providing a visual representation of which threats are more significant.
- **Data**: Each axis represents a different threat type, and the values indicate the threat proportion:
  - **Phishing**: 14.6%
  - **Insider**: 16.9%
  - **Malware**: 28.1%
  - **Hijacked Accounts**: 40.4%
- **Axes**: Each axis represents one type of threat, and the chart fills in to show the relative importance of each threat category.

These figures provide insights into security-related metrics, including anomaly detection, authentication efficiency, and threat sources.

Here are the details for each of the tables:

Table 1: Threat Sources

This table details the different threat sources and their respective percentages.

10.48047/jocaaa.2022.30.02.45

Threat Source	Percentage (%)
Malware	28.1
Phishing	14.6
Insider	16.9
Hijacked Accounts	40.4

- **Malware** accounts for 28.1% of the threats, making it the second-highest threat source.
- **Phishing** is responsible for 14.6% of the threats, representing a smaller portion of the total threats.
- **Insider threats** contribute 16.9% to the overall threat landscape.
- **Hijacked Accounts** pose the largest threat, representing 40.4% of the threats in the system, highlighting the significant risk of compromised accounts.

These tables provide valuable insights into how well different user groups are detecting anomalies and the major sources of threats within a security framework.

Discussion

The use of AI in Identity and Access Management (IAM) systems in cloud also caught the attention underpinning the increasing complexity and scale of today's enterprise security needs. Legacy IAM technologies like Role-Based Access Control (RBAC) have been front and centre on the security stage [1] in controlling access to enterprise resources for decades, but their limitations are being felt more acutely with today's complex cloud infrastructures (Bertino, Sandhu & Jajodia 2019). Artificial Intelligence-enhanced IAM within Oracle Cloud Security The discussion above covers the importance, challenges, advantages and impact of AI on security paradigms – check how we could apply all these to see what exactly happens in a smart future inside the field of Artificial Intelligence-aided Identity And Access Management?

Challenges with Traditional IAM Systems

Legacy IAM, RBAC included, has an approach to granting or denying access to a resource using fixed pre-defined roles. RBAC is suitable in static, stable environments, but lacks flexibility for the dynamic, cloud context where roles and authority to perform roles change frequently (Ferraiolo et al., 2007). Given that organizations are consuming cloud services and deploying hybrid IT environments, new IAM challenges like identity sprawl, unauthorized access and over-privileged users are too difficult to manage using traditional IAM (Chen, Zhao & Han 2018). Not

10.48047/jocaaa.2022.30.02.45

only that, but with the increasing requirement for real-time access management in cloud environments we are also moving to a security model which is more dynamic and anticipatory – something traditional IAM can't provide.

AI is thus becoming regarded as the solution to these challenges. AI can mitigate weaknesses of conventional IAM systems by means of ML models, anomaly detection techniques, and behavioral analytics via real time intelligence and alert from security threat and dynamic access control (Patel & Doshi, 2019). This is even more crucial for cloud-based IAM systems because the user patterns, roles and access logics are dynamic and likely changing over time (Zhang et al., 2019).

AI in Enhancing IAM Systems

IAM plus AI – opportunities A fusion of IAM and AI has some advantages such as: Improved security measures Automation for decision making Operating efficiency Anomaly access patterns respectively which is against historical user behavior and detects probable risk like insider(Volente) attack,insider(volute) threat,credential theft(insider),phishing etc could be detected by Artifact Model machine learning classifier Sharma & Chen (2020). They do not have to stop here, rather can use history of users to dynamically create access controls and minimize their exposure towards the stale/out-of-date permissions (Sharma & Chen, 2020). And then the last is behavioral analytics, because I can seek out anomalous behavior in real time that would enable me to take a more proactive approach around threat management.

Risk-Based and Adaptive Authentication One of the greatest advancements in AI-based IAM systems is that a Risk-Based Adaptive Authentication enables an AI logic to analyze each attempt made at access, measuring this risk in real time. Artificial Intelligence may assign a risk score to each request to enter based on user behavior, location and device. If the risk score is above a certain threshold, supplementary proof of identity (e.g. MFA) can be invoked to confirm that the user seeking access is indeed the person they say. (Oracle, 2020). It doesn't contribute only to make the context-aware access request more secure but also it increases users' feel that is at low resistance despite the door being not completely open.

10.48047/jocaaa.2022.30.02.45

Oracle delivers security and AI-driven Identity Management to its cloud Oracle's architectural design doesn't rely on separate IAM service components.

AI for Oracle Cloud Security also makes it easier to conform to regulation prior ((GDPR or HIPAA)) by offers transparent audit trail and real-time access event monitoring end-to-end visibility in the (Zhang & Li, 2019). With data more onus than ever, the AI-powered IAM systems will allow an enterprise to demonstrate compliance step by step in a shorter period of time with better security for that matter."

AI's Impact on Security Operations

Its power to auto perform repetitive IAM-tasks contributes in raising the operational performance of AI. By way of example, the process of add and droping users often consists manual and innacurate procedures. Nevertheless, AI will take over these operations through the use of pre-written rules or instantaneous feedback and in this way decrease chances of human errors and allow users to access only needed resources (Patel & Doshi, 2019).

Conclusion

One of the greatest strengths in AI for IAM solutions is through continuous detection of abnormal behaviors and access attempts. This is a great facility for safeguarding the corporation against insider threats and against phishing, credential hacking and other dodgy cyber doings that proliferate today (Zhang, Yu & Li, 2019). Artificial Intelligence (AI) based IAM systems can be learn and adopt to new patterns using old access details, and they are intelligent, proactive and reactive than conventional IAM solutions (Sharma & Chen, 2020). The very ‘dynamic’ aspect is that which makes AI/ML-based systems so interesting as part of cloud facilities, where both the scale and complexity and variety of both legitimate users as requests for access could quickly outpace what classic model might be capable to accommodate.

Furthermore, AE can also significantly automate a portion of the user management activities including provisioning, de-provisioning and policy enforcement that provides an opportunity for IT and security to work more with less administrative work (Bertino et al., 2019). As things stand, the severity of some processes, access control for example does anyone try and tell me with a straight face this area is perfectly enforced across all entities? Or hell, for some it just makes more sense to go proprietary because “compliance” …(read slows penetration down)

10.48047/jocaaa.2022.30.02.45

They even introduce a degree of manual error that will not transfer over all that well when an AI starts captaining the ship.

References

Alotaibi, S., & Al-Salman, A. (2020). *Identity and access management in cloud environments: Challenges and solutions*. Springer.

Bertino, E., Sandhu, R., & Jajodia, S. (2019). *Security and privacy in cloud computing: Challenges and opportunities*. Springer.

Chen, X., Zhao, L., & Han, Q. (2018). *AI-driven approaches for cloud security: An integrated view*. Springer.

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control*. Artech House.

Oracle. (2020). *Oracle Cloud Security and AI-enhanced identity management*. Oracle Corporation.

Patel, S., & Doshi, S. (2019). *AI for cybersecurity: Leveraging machine learning for security automation*. Wiley.

Sharma, P., & Chen, X. (2020). *Artificial intelligence in identity and access management: A review of current trends*. Springer.

Zhang, Y., Yu, H., & Li, Z. (2019). *Cloud computing and security issues: A survey of solutions*. Springer.