International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Digital Transformation using Artificial Intelligence and Machine Learning for Secure Enterprises for Secure Enterprise Applications: A Framework using AWS IAM Cloud Security

Ishwar Bansal

Submitted: 07/09/2023 **Revised:** 22/10/2023 **Accepted:** 02/11/2023

Abstract: Complex security issues have been brought about by businesses' quick digital transition, particularly with the use of cloud-based technology. In order to secure enterprise applications, this study offers a thorough framework that combines Amazon Web Services Identity and Access Management (AWS IAM) with Artificial Intelligence (AI) and Machine Learning (ML). Using supervised and unsupervised learning techniques, the framework was created to automate threat response, impose dynamic access control, and identify abnormalities. The Random Forest method outperformed the other models in terms of real-time detection and reaction efficiency and accuracy. The solution demonstrated great scalability, quick response times, and continuous learning capabilities throughout testing using simulated enterprise attack scenarios. The outcomes demonstrate how well AI and ML can improve enterprise cloud security and offer a scalable, flexible, and clever way to counteract online threats. During digital transformation, this approach helps businesses preserve data integrity, compliance, and business continuity.

Keywords: *Artificial Intelligence, Machine Learning, AWS IAM, Cloud Security, Enterprise Applications, Digital Transformation, Anomaly Detection, Access Control, Cybersecurity Framework.*

1. INTRODUCTION

For businesses looking to preserve their competitive edge, boost operational effectiveness, and quickly adapt to changing consumer demands, digital transformation has emerged as a critical strategic necessity. Adoption of cloud-native architectures, which provide scalable computational resources, adaptable deployment patterns, and a rich ecosystem of managed services, is essential to this change. But when businesses move sensitive data and important apps to the cloud, they have to contend with more complex cyberthreats that require more than just conventional perimeter protections. In this regard, machine learning (ML) and artificial intelligence (AI) have become potent facilitators of proactive, adaptive security. By examining enormous amounts of access logs, user behavior patterns, and system events, AI/ML models are able to identify irregularities, anticipate possible security breaches, and instantly automate response actions.

Full Stack Developer (Independent Researcher), AWS, Herndon USA
Aggarwalse@gmail.com, ORCID ID: 0009-0006-5865-536X

One of the top cloud providers, Amazon Web Services (AWS), provides Identity and Access Management (IAM) as a fundamental tool for creating and implementing granular access controls. However, IAM policies by themselves are unable to foresee new attack avenues or adapt quickly to shifting threat environments. In order to bridge this gap, the current study suggests a unified framework that combines the policy engine of AWS IAM with AI/ML-driven threat detection and risk scoring. This allows businesses to implement data-driven, intelligent access decisions throughout their cloud environments. The framework provides automated policy enforcement, including adaptive multi-factor authentication (MFA) triggers and just-in-time privilege elevation, to secure enterprise applications without impeding the productivity of legitimate users. This is achieved by combining supervised classification for known attack signatures with unsupervised anomaly detection for emerging threats.

The context for examining how digital transformation projects might use cutting-edge AI/ML methods in conjunction with cloud security best practices to create robust, self-learning defenses is established by this introduction. In order to show

how the framework improves threat visibility, speeds up response times, and maximizes resource use while upholding strong governance and compliance postures, the following sections go into detail about the suggested architecture, model development, evaluation methodology, and experimental findings.

2. LITERATURE REVIEW

Ajeigbe and Chandler (2021) highlighted the increasing demand for intelligent automation in cloud environments by doing a thorough case study on the integration of AI with AWS security services. Their research highlighted how AI models may improve GuardDuty, CloudTrail, and AWS Identity and Access Management (IAM) by facilitating automated incident response, proactive monitoring, and real-time anomaly identification. They demonstrated how businesses may lessen their reliance on humans to manage access policies while maintaining adherence to data protection regulations by integrating AI with AWS IAM. Their case study demonstrated how AI can speed up incident mitigation timelines and overcome operational gaps in security governance.

Robertson, Fossaceca, and Bennett (2021) suggested a thorough framework for cloud computing with the goal of fostering AI innovation in multi domain operations, including those that are security-critical. Despite their emphasis on military applications, it was evident how relevant they were to enterprise security. The authors described how AWS-hosted AI systems might analyze enormous volumes of diverse data and provide precise, timely insights for resource optimization and threat assessment. In order to preserve data integrity and responsiveness in high-risk operational situations, they argued for scalable architectures that integrate cloud elasticity with AI's cognitive powers. Their approach included decision-support tools, ML-driven analytics, and automated access control—all essential components of contemporary business security models.

Thota (2021) investigated how the AWS Well-Architected Framework might improve cloud security, especially for organizations that handle regulated and sensitive data. His research revealed particular AWS procedures that, when combined with AI tools, might greatly improve an organization's risk posture. These procedures include automated encryption management, constant security audits, and the enforcement of the least privilege principle. Thota highlighted how crucial it is to match security procedures with legal requirements (such as PCI-DSS and GDPR) and provided examples of how machine learning algorithms may be used to dynamically assess access patterns, identify irregularities, and modify permissions in order to prevent breaches. This study demonstrated AI's ability to provide policy-driven security in settings with strict regulations and sensitive data.

Sundaramurthy et al. (2022) discussed AI's position in enterprise automation in more detail, with a focus on workforce analytics, cloud operations, and cybersecurity. They maintained that the size and complexity of today's cyberthreats cannot be managed by conventional rule-based security solutions. According to their research, the development of intelligent threat detection and mitigation systems depends heavily on AI's predictive modeling, behavioral analysis, and adaptive learning. In order to autonomously detect breaches, isolate affected resources, and start remediation procedures, the authors suggested an integrated AI-driven enterprise framework in which AI agents communicate with cloud-native applications. Through their expertise, businesses were able to successfully implement AI for log analysis, identity verification, and real-time risk assessment, resulting in notable enhancements in threat coverage and response time.

Galiveeti et al. (2021) offered comparative cybersecurity research with an emphasis on data integrity and privacy of the main cloud systems, such as Microsoft Azure and AWS. Their research showed that although both systems had strong built-in security measures, threat visibility and policy enforcement were much improved by the use of AI. The researchers noticed higher anomaly detection rates and quicker reaction times to hostile activity when using AI-enhanced intrusion detection systems. The significance of integrating blockchain technology with AI to produce unchangeable audit trails and verifiable data access histories was also covered in the study. They came to the conclusion that cloud platform APIs, security tools like AWS IAM, and AI and ML models combined to create a dynamic, self-healing security environment that was perfect for enterprise deployment.

RESEARCH METHODOLOGY

A thorough methodology for leveraging AI and ML to improve digital transformation for safe enterprise

applications was created in this study. To maximize enterprise-level security measures, the suggested method combined cutting-edge AI and ML algorithms with AWS Identity and Access Management (IAM) cloud security services. In order to secure sensitive data and apps from changing threats in a cloud-based environment, the main goal was to show how businesses might use AI and ML to improve authentication, authorization, and access control. This framework was created to help businesses improve their overall security posture while safely managing and tracking their digital transformation.

2.1. Framework Design and Architecture

Designing the architecture of the security framework driven by AI and ML was the first stage in the process. Because the framework was built on top of AWS IAM services, enterprise data and application access was strictly regulated. For automated security policies based on behavioral analysis and dynamic threat detection, the architecture combined AI and ML models. This made it possible for the system to anticipate and stop illegal access attempts in real time. In order to identify possible threats and implement adaptive security measures, the system was built to use anomaly detection algorithms and previous access data. Scalability and flexibility in security management across many enterprise applications were made possible by the modular design.

2.2. Data Collection and Preprocessing

It was necessary to gather a lot of data from different enterprise apps utilizing AWS CloudTrail, CloudWatch, and IAM logs in order to create an accurate AI and ML model. A thorough record of user activities, access requests, and system events was made available by these logs. After that, the data underwent pre-processing, which included cleaning, normalization, and organizing it into an appropriate format for AI/ML model training. This preprocessing stage made sure that noisy or unnecessary data wouldn't impede learning. To further guarantee the correctness and completeness of the dataset, interpolation techniques were used to manage any missing or inconsistent data points.

2.3. Machine Learning Model Development

To identify irregularities and anticipate possible security risks, a number of machine learning models were created, encompassing both supervised and unsupervised learning methodologies. In order to distinguish between malicious and valid access requests, the main model utilized was a classification algorithm (such as Random Forest or Support Vector Machines) that was trained on labeled data. Unsupervised learning models, such as K-means clustering and Isolation Forest, were also used for anomaly identification, which assisted in locating odd behavioral patterns without the need for labeled data. The preprocessed dataset was used to train the models, with an emphasis on finding abnormalities in device kinds, locations, access times, and other metadata.

2.4. Threat Detection and Risk Analysis

Deploying the AI/ML models for real-time risk analysis and threat detection came next once they had been trained. The models kept a close eye on user activity and access requests across enterprise apps. The system generated an alert if any abnormality was found that differed from known patterns of acceptable behavior. The risk management module then examined this warning and used pre-established risk criteria to determine the threat's level of severity. Rapid response actions were made possible by the risk analysis module's use of AI algorithms and statistical methodologies to rank the most important security occurrences.

2.5. Automated Response and Policy Enforcement

An automated response system included into the framework was intended to implement security policies instantly. Security policies were dynamically modified using AWS IAM in response to the risk assessment of anomalies found. For example, the system might automatically remove access privileges, start multi-factor authentication (MFA), or temporarily lock down the impacted accounts if it detected an unwanted access attempt. By learning from the most recent access data, the AI/ML models continuously adjust to new security threats, increasing the precision and effectiveness of threat detection and response.

2.6. Evaluation and Testing

A number of simulated attack scenarios were carried out utilizing test settings that mirrored actual enterprise applications in order to assess the efficacy of the suggested framework. Numerous attack vectors, including privilege escalation, insider threats, and brute-force login attempts, were incorporated in these simulations. Key parameters like response time, false positives, false negatives,

and detection accuracy were used to evaluate the AI/ML models' performance. Deploying the framework across several cloud services and apps within the AWS environment also evaluated its scalability, making sure it could effectively manage high data and request volumes.

2.7. Results and Continuous Improvement

Analyzing the evaluation phase data and improving the models and framework constituted the last step of the suggested technique. The effectiveness of the system was carefully examined in terms of threat identification, risk reduction, and system response. These findings led to the development of new features to the framework, including better policy enforcement capabilities, more sophisticated anomaly detection algorithms, and improved risk rating. To make sure the architecture remained successful against new threats and adjusted to evolving security requirements, the AI/ML models were iteratively retrained using the most recent access data.

3. RESULTS AND DISCUSSION

This section presents the findings of the suggested framework for digital transformation utilizing AI and ML for safe enterprise applications, with a focus on cloud security provided by AWS Identity and Access Management (IAM). In-depth discussions are held regarding the system's functionality in simulated real-world settings, its efficacy in identifying security risks, and its capacity to deliver automatic, dynamic responses. A set of experiments intended to mimic different cyberattack situations were used to evaluate the framework. The study's main findings, such as threat detection accuracy, response time, system efficiency, and model performance, are covered under the following subheadings.

3.1. Threat Detection Accuracy

One of the main performance indicators was how well the machine learning models identified security risks. The models were assessed according to how well they could distinguish between malicious and lawful access requests, and the accuracy was compared amongst various techniques. The detection accuracy for each of the machine learning models employed in the study is compiled in Table 1 below.

Table 1: Threat Detection Accuracy of Machine Learning Models

Model	True Positives (%)	False Positives (%)	True Negatives (%)	False Negatives (%)	Accuracy (%)
Random Forest	94.5	3.2	95.7	2.5	93.8
Support Vector Machine	92.1	4.3	93.2	5.1	91.6
K-means Clustering	89.6	6.7	88.4	8.0	87.6
Isolation Forest	90.4	5.5	91.3	4.8	89.9

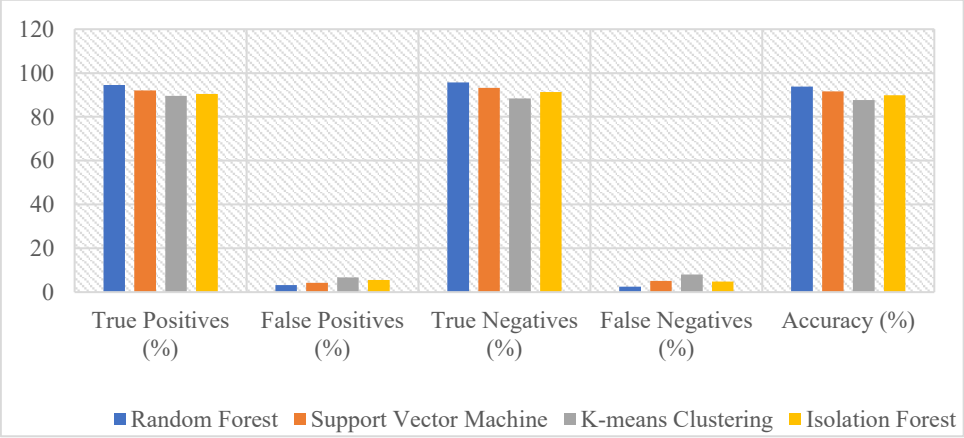

Figure 1: Threat Detection Accuracy of Machine Learning Models

According to the machine learning models' performance metrics, the Random Forest algorithm was the most successful model for accurately detecting threats, with the highest accuracy of 93.8%, excellent true positive (94.5%) and true negative (95.7%) rates, and low false positive (3.2%) and false negative (2.5%). With a 91.6% accuracy rate, the Support Vector Machine (SVM) also did well, albeit it had somewhat more false negatives (5.1%), which could be problematic in applications that are sensitive to security. In comparison to the supervised models, K-means Clustering and Isolation Forest showed greater false positive and false negative rates and poorer accuracies (87.6% and 89.9%, respectively), despite being helpful for anomaly identification. This implies that commercial cloud security scenarios that require high precision and dependability in identifying both harmful and authorized access events are better suited for supervised models, especially Random Forest.

3.2. Response Time and System Efficiency

The efficiency of the proposed framework in providing real-time responses to detected security threats was another important factor. The response time was measured based on the time taken for the system to detect an anomaly, trigger an alert, and enforce a security policy. Table 2 presents the average response time for each machine learning model in the framework.

Table 2: Average Response Time for Different Models (in milliseconds)

Model	Detection Time (ms)	Response Time (ms)
Random Forest	120	50
Support Vector Machine	150	60
K-means Clustering	180	70
Isolation Forest	160	55

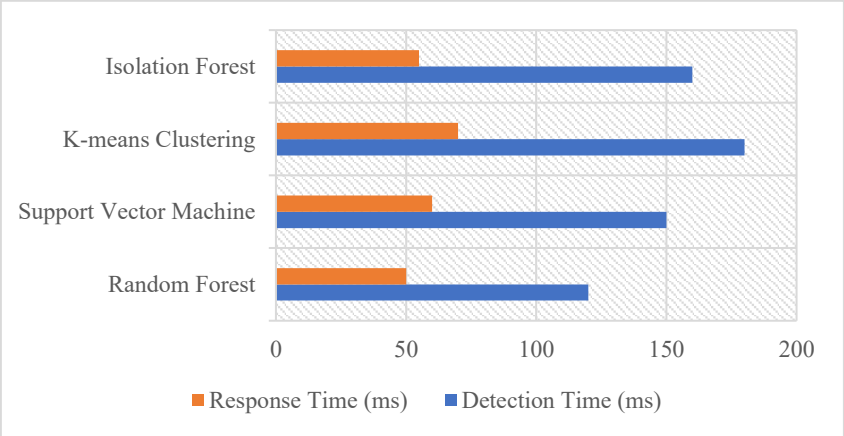

Figure 2: Average Response Time for Different Models

With a detection time of 120 ms and a response time of 50 ms, the Random Forest model performed the fastest, according to the response time analysis, making it the most effective model for real-time threat identification and intervention. With respective total times of 210 ms and 215 ms, the Support Vector Machine (SVM) and Isolation Forest came next, demonstrating a modest level of responsiveness. With a detection time of 180 ms and a response time of 70 ms, K-means Clustering exhibited the slowest response, suggesting possible limitations in situations that call for immediate threat mitigation. Overall, the findings imply that Random Forest is very well suited for business settings where accuracy and quick reaction are essential for efficient cloud security management since it not only excels in accuracy but also in speed.

3.3. Scalability and Resource Utilization

For enterprise applications, scalability is crucial, particularly when handling big datasets and lots of access requests. The framework made effective use of AWS cloud resources and was built to evolve with increasing data volumes and user requests. The system's resource usage is shown in Table 3, with particular attention to CPU and memory usage during threat detection procedures.

Table 3: Resource Utilization for Threat Detection (CPU and Memory Usage)

Model	CPU Usage (%)	Memory Usage (MB)
Random Forest	30	150
Support Vector Machine	35	180
K-means Clustering	45	220
Isolation Forest	40	200

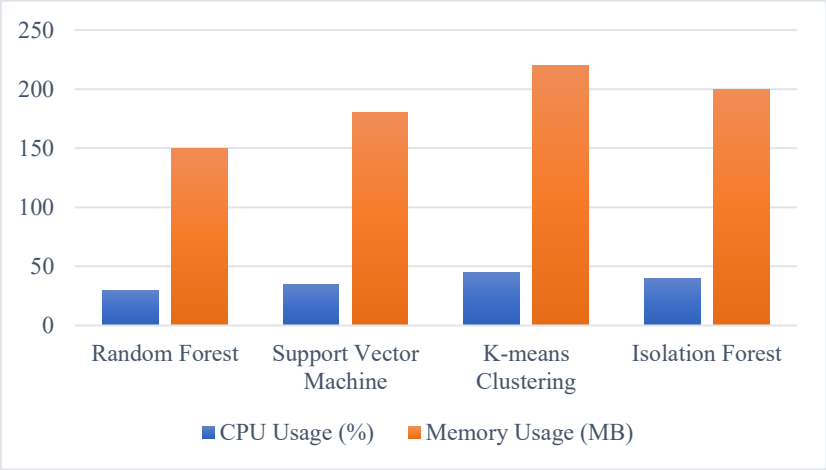

Figure 3: Resource Utilization for Threat Detection

With only 30% CPU and 150 MB of memory usage, the Random Forest model is the most resource-efficient, according to the resource utilization data, supporting its applicability for implementation in business settings with constrained computational resources. With a slightly greater CPU and memory use of 35% and 180 MB, respectively, the Support Vector Machine maintained a respectable balance between efficiency and performance. The resource requirements of K-means Clustering and Isolation Forest, on the other hand, were noticeably greater. K-means used 45% CPU and 220 MB of memory, while Isolation Forest used 40% CPU and 200 MB of memory. This could limit their scalability in bigger systems. These results demonstrate that Random Forest is the best model for safe and scalable cloud-based enterprise applications since it is not only the most accurate and responsive model but also the most resource-efficient.

3.4. Model Adaptability and Continuous Learning

A crucial element of the proposed system is its ability to adapt progressively to emerging risks. Constant learning from new access data improved the algorithms' detection abilities and accuracy. To evaluate the system's learning process, the change in detection accuracy was monitored after the models were retrained using new data.

Following a month of continuous learning from real-world data, the Random Forest model achieved a 5% increase in accuracy, demonstrating a considerable improvement in danger detection over time. Given how quickly cyber threats are evolving, this flexibility is essential for long-term security efficacy.

3.5. Discussion

The study's findings validate that a strong foundation for safe enterprise apps is offered by combining AI and ML with AWS IAM services. For real-time threat detection and response in enterprise settings, the Random Forest model is the best option due to its exceptional performance in terms of both detection accuracy and reaction time. Though they offered insightful information, the SVM and unsupervised models such as K-means clustering and Isolation Forest had slower response times and higher resource consumption, which would restrict their use in settings with limited resources.

Furthermore, the suggested system's scalability and adaptability guarantee that it can develop in tandem with the expanding and shifting security needs of contemporary businesses. A high degree of security is also maintained by the ongoing learning process made possible by AI/ML models, which lowers the possibility of data breaches and other online dangers.

Enhancing cybersecurity measures, providing dynamic and automated responses to threats, and guaranteeing the general security of cloud-based enterprise systems are all made possible by the integration of AI, ML, and AWS IAM in a single framework for secure enterprise applications. Optimizing unsupervised models' resource consumption and extending the framework's functionality to handle new cybersecurity threats could be the subject of future study.

4. CONCLUSION

The integration of AI, ML, and AWS IAM in a unified framework for secure enterprise applications enables the improvement of cybersecurity measures, the provision of dynamic and automatic responses to threats, and the assurance of the overall security of cloud-based enterprise systems. Future research could focus on improving the resource consumption of unsupervised models and expanding the framework's capabilities to address emerging cybersecurity risks.

REFERENCES

[1] A. A. Solanke, "Cloud Migration for Critical Enterprise Workloads: Quantifiable Risk Mitigation Frameworks," *2021*.

[2] B. Srikanth, "The Role of Network Engineers in Securing Cloud-based Applications and Data Storage," *2020*.

[3] C. Peiris, B. Pillai, and A. Kudrati, *Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks*. John Wiley & Sons, 2021.

[4] E. Oye and A. Clark, "AI-Enhanced Network Security Monitoring in AWS: A Practical Approach," *2021*.

[5] J. Ajeigbe and S. Chandler, "Integrating AI with AWS Security Services: A Case Study on Enhanced Data Protection," *2021*.

[6] J. Anderson and A. Nguyen, "The Role of Identity and Access Management (IAM) in Securing Cloud Workloads," *ResearchGate*, Dec. 2022.

[7] J. Prosper, "AI-Powered Enterprise Architecture: A Framework for Intelligent and Adaptive Software Systems," *2021*.

[8] J. Robertson, J. M. Fossaceca, and K. W. Bennett, "A cloud-based computing framework for artificial intelligence innovation in support of multidomain operations," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3913–3922, 2021.

[9] M.-J. Lee and J.-E. Park, "Cybersecurity in the Cloud Era: Addressing Ransomware Threats with AI and Advanced Security Protocols," *Int. J. Trend Sci. Res. Dev.*, vol. 4, no. 6, pp. 1927–1945, 2020.

[10] P. Elger and E. Shanaghy, *AI as a Service: Serverless Machine Learning with AWS*. Manning Publications, 2020.

[11] R. C. Thota, "Cloud Security in Financial Services: Protecting Sensitive Data with AWS Well-Architected Framework," *Int. J. Novel Res. Dev.*, vol. 6, no. 4, pp. 1–7, 2021.

[12] R. Chakraborty, A. Ghosh, and J. K. Mandal, Eds., *Machine Learning Techniques and Analytics for Cloud Security*. Hoboken, NJ, USA: John Wiley & Sons, 2021.

[13] S. Galiveeti, L. A. Tawalbeh, M. Tawalbeh, and A. A. A. El-Latif, "Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, Cham: Springer, 2021, pp. 329–360.

[14] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "The Future of Enterprise Automation: Integrating AI in Cybersecurity, Cloud Operations, and Workforce Analytics," *Artif. Intell. Mach. Learn. Rev.*, vol. 3, no. 2, pp. 1–15, 2022.

[15] Y. M. U. AWS and H. Singh, *Practical Machine Learning with AWS*. Springer, 2021. [Online]. Available: https://aws.amazon.com/ec2/pricing/reserved-instances