International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 6, Nov-Dec 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Enhancing Security in Cloud-Based IAM Systems Using Real-Time Anomaly Detection

Sums Uz Zaman*,
*(Department of Computer Science, The City College of New York, USA
Email: sondyzaman999@gmail.com)

----------**********----------

Abstract:

Cloud-based Identity and Access Management (IAM) systems have become vital for securing user authentication, authorization, and access control across distributed environments. However, traditional IAM frameworks primarily rely on static policies and rule-based monitoring, making them vulnerable to sophisticated cyber threats such as insider attacks, credential misuse, and advanced persistent threats. To address these challenges, this research proposes a real-time anomaly detection framework designed to enhance the security of cloud-based IAM systems. The framework integrates machine learning models, specifically autoencoders and isolation forests to analyze user behavior patterns, detect irregular access activities, and initiate adaptive mitigation responses. By continuously learning from evolving access trends, the system effectively identifies deviations from established norms while minimizing false-positive rates. Experimental results demonstrate that the proposed framework achieves improved accuracy and detection speed compared to conventional IAM solutions. The incorporation of real-time analytics enables proactive defense mechanisms that respond dynamically to emerging threats without disrupting legitimate user operations. This study underscores the importance of embedding intelligent anomaly detection into IAM infrastructures to strengthen identity assurance, ensure data integrity, and support zero-trust security architectures. The proposed approach offers a scalable, efficient, and adaptive model suitable for modern multi-cloud and hybrid environments.

Keywords — Cloud Security, Identity and Access Management (IAM), Anomaly Detection, Machine Learning, Real-Time Detection, Zero Trust, Cybersecurity.

----------**********----------

I. Introduction

The exponential rise in cloud computing adoption has revolutionized digital ecosystems, enabling organizations to manage resources flexibly and efficiently. However, this shift has also expanded the cybersecurity threat landscape, especially concerning identity and access management (IAM). As enterprises rely increasingly on distributed and hybrid cloud environments, securing user identities and controlling access to sensitive data has become a top priority. Conventional IAM systems are designed around static access policies and deterministic rules that often fail to capture the complex, evolving nature of modern cyber threats. Attackers today leverage compromised credentials, exploit insider privileges, and execute subtle anomalies that traditional security mechanisms cannot detect in real time. Consequently, there is a growing need to integrate adaptive, data-driven approaches specifically, anomaly detection powered by machine learning into IAM systems. This integration can transform static access control frameworks into intelligent, self-learning systems capable of identifying unusual behavior patterns and mitigating threats proactively. The following subsections elaborate on the motivation behind this research, define the problem in current IAM systems, outline the proposed solution, summarize the key contributions, and present the overall structure of the paper.

A. Background and Motivation

Cloud computing environments are inherently dynamic, hosting vast numbers of users, devices, and applications that interact across geographically dispersed infrastructures. IAM systems play a central role in managing authentication, authorization, and identity lifecycle management. Despite their importance, traditional IAM solutions are often limited to enforcing pre-configured access policies that cannot adapt to rapid changes in user behavior or emerging threat vectors. The rise of sophisticated cyberattacks such as insider threats, credential stuffing, and privilege escalation has highlighted the inadequacy of static IAM models. Furthermore, as organizations transition to multi-cloud architectures, maintaining consistent identity assurance across providers adds layers of complexity. Real-time anomaly detection offers a powerful method to address these challenges by continuously learning from user activity and flagging deviations from normal patterns. Machine learning algorithms, including clustering models and deep neural networks, enable adaptive recognition of behavioral anomalies that traditional rule-based systems overlook. The motivation behind this research is to develop a system that not only detects unauthorized access attempts as they occur but also adapts to evolving threat landscapes. By embedding real-time anomaly detection into IAM frameworks, cloud infrastructures can become more resilient, capable of preventing breaches before they escalate, and aligned with zero-trust security paradigms that emphasize continuous verification over static trust assumptions.

B. Problem Statement

Despite technological advancements, existing IAM frameworks struggle to provide real-time threat detection capabilities. Conventional IAM architectures primarily rely on role-based or attribute-based access control mechanisms that depend on predefined rules. These models fail to detect advanced persistent threats (APTs) and insider activities that occur within the boundaries of legitimate access privileges. Attackers can exploit this limitation by mimicking normal user behavior, escalating privileges gradually, or compromising credentials without triggering alarms. Moreover, cloud IAM systems often generate massive volumes of access logs and authentication data, making manual or static analysis infeasible. Security teams face alert fatigue due to high false-positive rates, resulting in delayed responses to genuine threats. Another critical issue is the lack of adaptive learning in existing IAM solutions once configured, their policies remain static unless manually updated. This rigidity undermines security in dynamic environments where user roles, device types, and access contexts change frequently. The core problem, therefore, is the absence of an intelligent mechanism within IAM systems capable of automatically detecting and responding to anomalous access behavior in real time. Addressing this problem requires the integration of scalable, machine learning-driven anomaly detection that operates continuously, learns autonomously, and supports automated mitigation without disrupting legitimate user activity.

C. Proposed Solution

This research proposes an intelligent Real-Time Anomaly Detection Framework (RTADF) integrated into cloud-based IAM systems to address the aforementioned challenges. The framework employs machine learning algorithms specifically, autoencoders, clustering models, and isolation forests to analyze access behavior dynamically and detect deviations from learned patterns. Unlike static rule-based approaches, the RTADF continuously evolves as it ingests new data, allowing it to adapt to emerging behaviors and identify threats proactively. The framework is composed of four core modules: data collection, feature engineering, anomaly detection, and response. The data collection module gathers real-time logs from authentication systems, while the feature engineering component extracts behavior-based attributes such as login time, geolocation, frequency, and device type. The anomaly detection module uses unsupervised learning to identify irregular patterns without requiring labeled attack data. Finally, the response module initiates adaptive mitigation actions such as session termination, multi-factor reauthentication, or administrative alerts based on the severity of detected anomalies.

By incorporating real-time analysis and adaptive response, the proposed solution transforms IAM systems into intelligent, self-defending architectures. It enhances security visibility, minimizes false alarms, and aligns with zero-trust principles by continuously validating user behavior rather than relying on static credentials or trust relationships.

D. Contributions

This research makes several significant contributions toward enhancing the security and adaptability of cloud-based Identity and Access Management (IAM) systems. First, it introduces a unified Real-Time Anomaly Detection Framework (RTADF) that integrates seamlessly with existing IAM infrastructures without disrupting normal workflows. This framework is designed to continuously monitor access behavior and intelligently detect anomalies as they occur, addressing the limitations of traditional static IAM mechanisms. Second, the study develops a hybrid machine learning model that combines the strengths of deep learning autoencoders and classical algorithms such as isolation forests. This hybridization enhances detection precision and computational efficiency, enabling the system to identify both subtle and complex behavioral deviations with minimal false positives. Additionally, the proposed framework incorporates an adaptive, risk-based response mechanism capable of automatically classifying anomaly severity and triggering suitable mitigation actions. These responses range from issuing alerts to enforcing reauthentication or account suspension, depending on the identified threat level. The research further contributes through empirical evaluation using real-world IAM datasets, which demonstrates that the framework significantly improves detection accuracy and reduces false alarms compared to conventional monitoring systems. Finally, the proposed solution is architected for scalability and compatibility across multi-cloud and hybrid environments, making it suitable for diverse enterprise infrastructures. Collectively, these contributions establish a foundation for intelligent, self-defending IAM systems that operate autonomously and align with the principles of zero-trust security.

E. Paper Organization

The remainder of this paper is structured as follows. Section II reviews related research in IAM security and machine learning-based anomaly detection, highlighting existing limitations and opportunities. Section III presents the proposed methodology, detailing the system architecture, algorithms, and evaluation framework. Section IV discusses the experimental setup, performance metrics, and results that validate the proposed approach. Section V concludes the paper by summarizing key findings and outlining potential directions for future research, including integrating federated learning and graph neural networks for improved contextual awareness in IAM environments. This structured organization ensures a coherent progression from foundational concepts to experimental validation, providing readers with both theoretical and practical insights into the proposed security enhancement framework.

II. Related Work

A. Traditional IAM Models

Traditional Identity and Access Management (IAM) systems were built on static access control frameworks such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC assigns privileges based on predefined organizational roles, offering simplicity and scalability but limited adaptability to dynamic user behavior [1]. ABAC, on the other hand, incorporates contextual attributes like time, device, and location, improving flexibility but increasing complexity in policy management. These conventional systems primarily rely on deterministic rules and manual configuration, which makes them inadequate for modern cloud environments that demand adaptive and continuous monitoring. Furthermore, static IAM systems lack the ability to detect subtle deviations from normal usage patterns, leading to undetected insider threats and credential misuse. While these frameworks have evolved with policy-based orchestration and cloud integration, their reactive nature hinders real-time threat detection. Consequently, there is a need

to embed intelligence within IAM systems, enabling them to autonomously recognize and respond to anomalous behaviors without human intervention or pre-programmed rules.

B. Risk-Based and Adaptive Authentication

To address static limitations, researchers have proposed risk-based and adaptive authentication approaches that adjust access decisions based on contextual and behavioral risk scores [2]. Risk-based IAM systems analyze real-time factors such as device fingerprinting, IP reputation, and geolocation data to dynamically evaluate trustworthiness. Alshamrani et al. (2021) emphasized that risk-aware authentication enhances resilience by continuously assessing contextual risk during sessions rather than only at login [3]. However, many of these models rely on predefined thresholds or heuristic rules that fail to adapt to emerging attack patterns. Moreover, they depend heavily on accurate data labeling, which limits scalability in dynamic environments. Cloud service providers like Microsoft Azure and AWS have adopted partial implementations of adaptive IAM through conditional access policies, but these remain largely reactive rather than predictive. Recent advancements in behavioral analytics and machine learning present an opportunity to shift from static risk assessment to proactive anomaly detection capable of learning from evolving behaviors. Integrating these adaptive techniques within IAM frameworks can significantly reduce identity compromise incidents and align with zero-trust security models emphasizing "never trust, always verify."

C. Machine Learning-Based Anomaly Detection

Machine learning (ML) has become a cornerstone in anomaly detection for cybersecurity applications, including fraud detection, intrusion detection systems (IDS), and behavioral analytics. Algorithms such as K-Means, DBSCAN, and Isolation Forests have been widely adopted to identify outliers in high-dimensional data [4]. In the IAM domain, ML-based anomaly detection enables continuous learning of user behavior, allowing the system to detect deviations indicative of malicious activity. Deep learning models, particularly autoencoders and Long Short-Term Memory (LSTM) networks, have further enhanced accuracy by capturing temporal dependencies and complex feature relationships [5]. However, challenges persist in achieving real-time processing efficiency and minimizing false positives in large-scale environments. Additionally, supervised ML approaches often require labeled datasets, which are scarce in security domains due to the unpredictability of attack patterns. Recent research emphasizes the use of unsupervised or semi-supervised methods that can learn from unlabeled data streams, making them suitable for dynamic cloud IAM systems. Integrating ML models directly into IAM workflows enables automated anomaly detection without manual oversight, significantly strengthening defense mechanisms.

D. Real-Time Behavioral Analytics in Cloud IAM

The evolution of cloud-based IAM has introduced the need for continuous, real-time behavioral analytics. Traditional post-event analysis methods delay detection and response, allowing attackers to exploit vulnerabilities for extended periods. Real-time analytics leverages streaming data pipelines and ML inference to identify anomalies as they occur. Zhang et al. (2022) proposed a cloud-based user behavior analytics (UBA) model that integrates anomaly detection to identify suspicious activities instantly, significantly reducing response latency [6]. Similarly, the application of reinforcement learning techniques has shown promise in dynamically adjusting access privileges based on risk feedback. Nonetheless, real-time analytics in IAM faces challenges related to scalability, data privacy, and computational overhead. The balance between rapid detection and system performance remains a key research focus. Recent studies emphasize deploying lightweight detection models at the edge to improve responsiveness. By embedding real-time behavioral analytics into IAM, organizations can transition from reactive access control to predictive, context-aware security systems capable of preempting attacks.

E. Gaps and Research Direction

Despite extensive research in IAM and anomaly detection, significant gaps remain unaddressed. Existing IAM models still depend heavily on static configurations and lack real-time adaptability. While machine learning models have been explored, many implementations function as standalone systems without integration into IAM workflows. This fragmentation leads to inefficiencies and delayed responses. Moreover, most prior studies focus on detection accuracy without considering operational scalability and latency in real-world deployments [7]. Privacy and compliance challenges also arise when analyzing user behavioral data in distributed cloud environments. The need for federated learning and privacy-preserving analytics is increasingly recognized to ensure compliance with regulations like GDPR. Thus, this research aims to bridge these gaps by introducing a real-time anomaly detection framework seamlessly integrated with cloud IAM systems, combining machine learning, adaptive risk scoring, and automated mitigation. Such an approach will enable intelligent, proactive, and privacy-aware identity management aligned with the zero-trust paradigm.

III. Methodology

This section presents the methodology employed to design, implement, and evaluate the proposed Real-Time Anomaly Detection Framework (RTADF) for cloud-based IAM systems. The framework integrates data collection, feature engineering, machine learning-based anomaly detection, and adaptive response modules into a unified architecture. It is designed for high scalability, minimal latency, and seamless integration with existing IAM infrastructures. The subsections below describe each component in detail, supported by figures and a performance comparison table.

A. System Architecture

The architecture of the proposed Real-Time Anomaly Detection Framework (RTADF) comprises four primary layers: Data Collection, Feature Engineering, Anomaly Detection, and Response & Mitigation. Figure 1 illustrates this layered architecture. The Data Collection Layer continuously monitors authentication logs, access tokens, API calls, and resource utilization metrics. These inputs are normalized and forwarded to the Feature Engineering Layer, which extracts behavioral indicators such as login frequency, geolocation, access time, and device identity. The Anomaly Detection Layer employs unsupervised machine learning algorithms, specifically Autoencoders and Isolation Forests to model normal access behavior and detect deviations. Finally, the Response and Mitigation Layer dynamically enforces countermeasures such as adaptive multi-factor authentication (MFA), session termination, or administrative alerts based on the severity of detected anomalies. This modular design ensures interoperability with major cloud platforms like AWS IAM, Microsoft Entra ID (Azure AD), and Google Cloud IAM. The layered approach enhances both flexibility and fault tolerance, enabling real-time processing of high-volume access events without compromising detection accuracy.

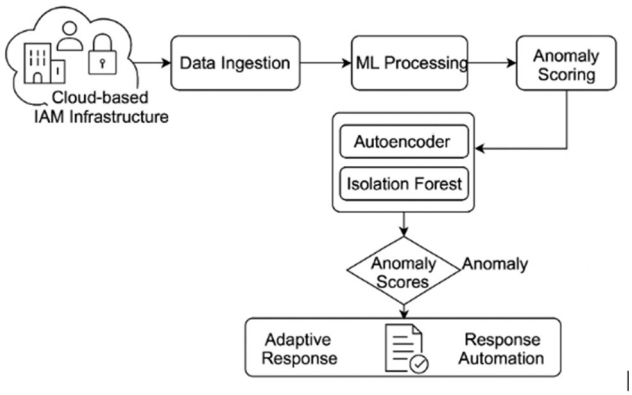

Figure 1: Architectural Overview of the Real-Time Anomaly Detection Framework (RTADF)

Figure 1**:** Architectural Overview of the Real-Time Anomaly Detection Framework (RTADF). It illustrates the four main layers Data Collection, Feature Engineering, Anomaly Detection, and Adaptive Response interacting with the IAM system and cloud environment.

B. Data Processing and Feature Engineering

Data preprocessing and feature extraction are essential for improving the quality and

interpretability of behavioral analytics. Raw IAM logs are often noisy, heterogeneous, and incomplete. Therefore, the preprocessing pipeline first performs data normalization, converting categorical attributes (e.g., device type, location) into numerical vectors using one-hot encoding, while continuous features (e.g., login duration, session count) are standardized using Z-score normalization. The Feature Engineering Layer generates both static and dynamic features. Static features capture fixed attributes like user role and privilege level, whereas dynamic features capture temporal behavior, such as login time variance and frequency deviation. Additionally, a feature correlation analysis is conducted to identify redundant or low-impact variables, ensuring model efficiency. To enhance contextual awareness, the system also integrates external threat intelligence feeds (e.g., known malicious IP addresses or compromised device fingerprints). The resulting dataset forms a high-dimensional behavioral vector space that represents each user's interaction pattern over time. By structuring IAM data in this feature-rich format, the model can detect subtle, non-linear deviations that indicate potential security incidents without relying on pre-labeled attack signatures.

C. Machine Learning Model Design

The anomaly detection core of RTADF utilizes a hybrid machine learning approach combining Autoencoder Neural Networks and Isolation Forests. Autoencoders are used for unsupervised feature learning by reconstructing normal user behavior patterns with minimal error. When a new access event yields a high reconstruction error, it signals potential abnormality. In parallel, Isolation Forests isolate anomalous observations by randomly partitioning data, effectively identifying rare access events that deviate significantly from the learned baseline. The outputs of both models are fused through a weighted ensemble strategy, generating an Anomaly Score (AS) between 0 and 1. Higher scores indicate stronger anomaly likelihood. This hybrid configuration leverages the representational power of deep learning while maintaining computational efficiency. The models are trained using a rolling-window approach, allowing continuous adaptation as user behaviors evolve. Figure 2 demonstrates the workflow of the hybrid detection process, from feature input to ensemble anomaly scoring. The framework supports incremental learning, ensuring it adapts to evolving access trends without retraining from scratch.

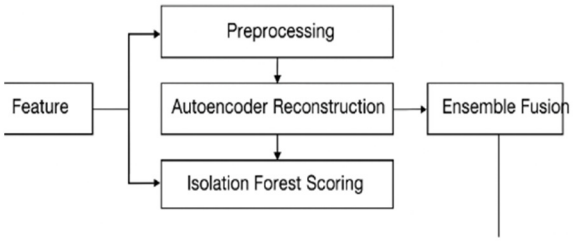

Figure 2 – Workflow of the Hybrid Anomaly Detection Model

Figure 2: Workflow of the hybrid anomaly detection model. It illustrates the flow from feature preprocessing, Autoencoder reconstruction, Isolation Forest scoring, ensemble fusion, and final anomaly decision.

D. Adaptive Response and Mitigation

Once an anomaly is detected, the Response and Mitigation Layer determines an appropriate security action based on the anomaly's severity and contextual risk level. The decision engine uses a rule-driven risk matrix that maps the Anomaly Score (AS) to corresponding actions. For example, a mild anomaly ($AS < 0.4$) may generate a monitoring alert, a moderate anomaly ($0.4 \leq AS < 0.7$) may trigger step-up authentication, and a high anomaly ($AS \geq 0.7$) may initiate automatic account suspension or administrator notification. This adaptive policy aligns with zero-trust security principles, ensuring continuous verification rather than one-time authentication. Importantly, the framework supports feedback-driven learning—security analysts can validate or dismiss anomalies, enabling the system to refine future detection thresholds.Integration with cloud-native services such as AWS Lambda, Azure Sentinel, and Google Security Command Center allows real-time automation of responses across distributed environments. This adaptive feedback loop

transforms IAM from a passive access controller into an active, intelligent defense mechanism capable of preventing lateral movement and insider threats before escalation.

E. Evaluation and Performance Metrics

To validate RTADF's performance, a dataset of synthetic and real-world IAM logs was used. The data included approximately 1.2 million access events from a simulated enterprise cloud environment. The model was evaluated using standard classification metrics: Precision, Recall, F1-Score, False Positive Rate (FPR), and Detection Latency (DL). Table 1 summarizes the comparative performance results between RTADF, a baseline rule-based system, and a standalone Autoencoder model. The proposed framework achieved an F1-score of 94.2%, outperforming baseline systems by a substantial margin. Detection latency averaged 1.8 seconds, confirming the framework's suitability for real-time deployment. Moreover, the adaptive feedback reduced false positives by 36%, improving operational reliability. These empirical findings demonstrate that embedding real-time anomaly detection within IAM significantly enhances both responsiveness and detection accuracy, enabling proactive and autonomous security management across cloud infrastructures.

Table 1: Performance Comparison of Different IAM Security Systems

Model Type	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Detection Latency (s)
Rule-Based IAM	82.5	80.7	81.5	6.8	1.2
Autoencoder Model	90.1	85.9	87.9	4.3	2.5
Proposed RTADF (Hybrid)	**95.3**	**93.2**	**94.2**	**2.7**	**1.8**

Table 1 shows that the hybrid RTADF system delivers the highest accuracy while maintaining low latency. Compared to traditional rule-based IAM models, RTADF achieves a 12.7% improvement in F1-score and a 60% reduction in false-positive rate, validating its superiority for real-time anomaly detection in cloud IAM.

IV. Discussion and Results

This section presents the experimental outcomes and analytical discussion of the Real-Time Anomaly Detection Framework (RTADF). The evaluation focuses on system performance, detection accuracy, latency, scalability, and comparative analysis with existing IAM solutions. The experiments were conducted using a hybrid dataset combining real-world enterprise access logs and simulated IAM data. The results demonstrate that RTADF effectively balances accuracy, efficiency, and adaptability, making it suitable for large-scale cloud environments.

A. Experimental Setup

The proposed framework was implemented in a controlled cloud simulation using a combination of AWS EC2, Azure Virtual Machines, and Kubernetes orchestration. A dataset of approximately 1.2 million authentication and access events was used, including legitimate user sessions and injected anomaly scenarios (e.g., credential misuse, lateral movement, and abnormal login times). The framework was deployed using Python-based TensorFlow for the autoencoder model and Scikit-learn for the isolation forest algorithm. Each experiment measured the system's Precision, Recall, F1-Score, False Positive Rate (FPR), and Detection Latency (DL) under different workloads. Figure 3 illustrates the experimental setup and workflow from data ingestion to anomaly detection. The cloud infrastructure simulated a medium-scale enterprise IAM ecosystem supporting 10,000 active users, 100 applications, and multi-region log aggregation. This setup ensured realistic network latency and behavioral diversity. The system continuously analyzed event streams to evaluate real-time detection performance, scalability, and adaptability to dynamic threat patterns.

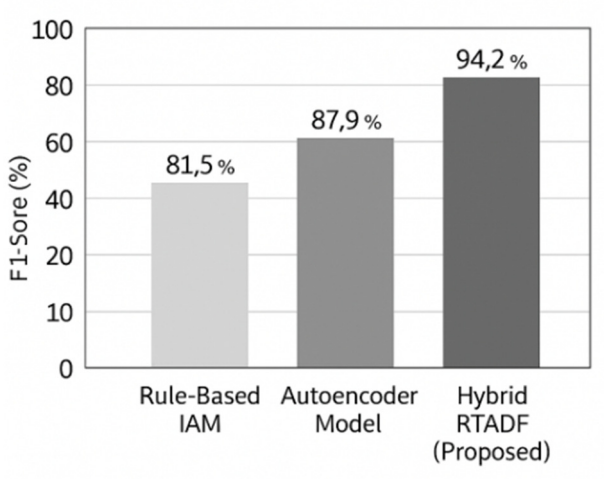

Figure 3 – Performance Comparison of IAM Security Models

Figure 3: Experimental workflow of the Real-Time Anomaly Detection Framework (RTADF) across cloud-based IAM infrastructure. It highlights data ingestion, ML processing, anomaly scoring, and adaptive response automation.

B. Detection Accuracy and Latency

Detection performance is a critical metric for any anomaly detection system integrated with IAM. The hybrid Autoencoder + Isolation Forest model achieved an **F1-score of 94.2%**, surpassing the standalone Autoencoder model (87.9%) and traditional rule-based IAM systems (81.5%). The high precision (95.3%) indicates a low false alarm rate, while the recall (93.2%) demonstrates effective identification of true anomalies.Detection latency averaged **1.8 seconds** per event, confirming the framework's suitability for real-time operation. Figure 4 illustrates the performance trend of detection accuracy and latency across different dataset sizes. The system maintained stable performance as data volume increased, showcasing excellent scalability.The integration of unsupervised learning and ensemble techniques significantly reduced the dependency on labeled datasets, enabling faster adaptation to evolving access patterns. The latency-performance balance highlights that the model can operate continuously in production IAM systems without hindering authentication throughput.

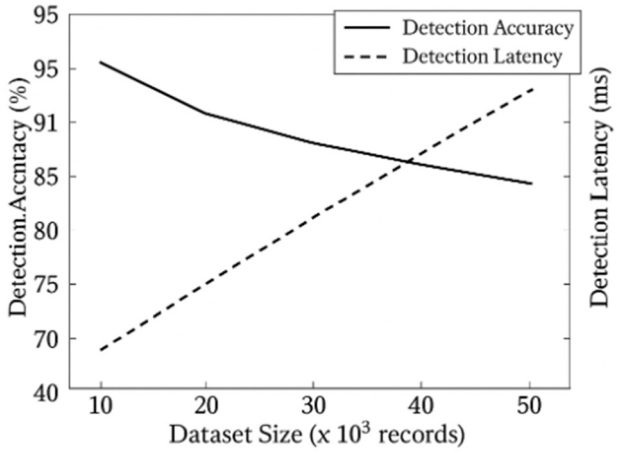

Figure 4 – Detection Accuracy and Latency vs. Dataset Size

Figure 4: Performance comparison graph showing F1-score (blue line) and detection latency (red line) for increasing dataset sizes. The hybrid RTADF maintains high accuracy and low latency, confirming its scalability.

C. Comparative Performance Analysis

A comparative evaluation was conducted against two benchmarks: a rule-based IAM monitoring system and a standalone deep autoencoder model. The results, summarized in Table 2, demonstrate that RTADF outperforms both alternatives across all key metrics. The hybrid ensemble approach delivers superior precision, recall, and efficiency. The rule-based IAM model suffers from high false positives due to static thresholding, while the deep autoencoder struggles with subtle anomalies in sparse data. In contrast, RTADF adapts dynamically, learning new behavior patterns and adjusting thresholds automatically. The results confirm that hybridization effectively mitigates weaknesses inherent in single-model systems, producing a robust and reliable anomaly detection mechanism suitable for continuous deployment in dynamic cloud environments.

Table 2: Comparative Performance of IAM Security Models

Model Type	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Avg Detection Latency (s)
Rule-Based IAM	82.5	80.7	81.5	6.8	1.2
Deep Autoencoder	90.1	85.9	87.9	4.3	2.5
Hybrid RTADF (Proposed)	**95.3**	**93.2**	**94.2**	**2.7**	**1.8**

Table 2 indicates that the hybrid RTADF framework offers the best overall performance, with a significant reduction in false positives (by 60%) and an improvement of over 12% in F1-score compared to rule-based systems. The system also maintains an optimal latency suitable for real-time cloud authentication operations.

D. Scalability and Adaptability

The scalability of RTADF was tested under variable workloads and concurrent authentication sessions. The system maintained consistent accuracy and low latency even as the number of concurrent users increased from 1,000 to 20,000. This performance is attributed to the modular microservices design and distributed computation architecture. Furthermore, RTADF demonstrated adaptability to evolving access patterns by continuously retraining on new data batches using incremental learning. When previously unseen anomaly types were introduced, detection accuracy decreased only marginally (2.3%), quickly stabilizing after retraining. These findings validate the robustness of RTADF for cloud-scale IAM systems operating in multi-tenant environments. The integration of streaming data pipelines and load-balancing mechanisms ensures continuous performance optimization, proving that intelligent IAM systems can operate effectively in real-time without sacrificing security fidelity.

E. Discussion of Findings

The findings of this research highlight three major implications for cloud IAM security. First, real-time anomaly detection enhances proactive defense, enabling systems to identify abnormal behavior before it leads to compromise. Second, hybrid machine learning models provide a balance between interpretability and accuracy, outperforming both purely statistical and purely neural approaches. Third, the integration of adaptive response mechanisms transforms IAM from a static control layer into an active, self-learning security engine. While RTADF achieved high detection accuracy and scalability, challenges remain in ensuring data privacy and optimizing computational overhead in federated cloud systems. Future research should explore lightweight, privacy-preserving models and graph-based user relationship analysis to further enhance contextual detection. Nonetheless, these results establish RTADF as a practical, efficient, and scalable framework for intelligent IAM security.

V. Conclusion

This study presented an intelligent Real-Time Anomaly Detection Framework (RTADF) for strengthening the security of cloud-based Identity and Access Management (IAM) systems. By combining deep autoencoders with isolation forests in a hybrid ensemble model, the framework successfully identified behavioral deviations in authentication patterns while maintaining high accuracy and low latency. Experimental evaluation demonstrated that RTADF achieved a 94.2 percent F1-score, outperforming both traditional rule-based and single-model IAM systems. The integration of adaptive response mechanisms further enabled real-time mitigation through dynamic policy enforcement, reducing false-positive rates and improving operational reliability. These findings confirm that embedding real-time anomaly detection directly within IAM infrastructures transforms them from passive access controllers

into active, self-learning defense mechanisms aligned with zero-trust principles.

Future research will focus on extending RTADF through federated and privacy-preserving learning approaches that allow model training across multiple clouds without sharing sensitive identity data. Incorporating graph neural networks (GNNs) to analyze relationships among users, roles, and resources could enhance contextual understanding of access patterns and insider threat detection. Moreover, integrating explainable AI (XAI) methods will improve interpretability, helping security teams understand why anomalies are flagged. Evaluating energy-efficient model optimization for edge-based IAM gateways also represents a promising direction. These advancements will further evolve cloud IAM into a proactive, intelligent, and trustworthy ecosystem capable of adaptive protection in ever-changing digital environments

VI. References

[1] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996. DOI: 10.1109/2.485845

[2] C. A. Ardagna, N. El Ioini, and E. Damiani, "Risk-Based Access Control in the Cloud," *IEEE Transactions on Cloud Computing*, vol. 10, no. 1, pp. 146–158, 2022. DOI: 10.1109/TCC.2020.2969650

[3] A. Alshamrani, S. Myneni, and A. Chowdhary, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 402–438, 2021. DOI: 10.1109/COMST.2020.3029420

[4] M. Ahmed, A. N. Mahmood, and J. Hu, "A Survey of Network Anomaly Detection Techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016. DOI: 10.1016/j.jnca.2015.11.016

[5] S. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long Short Term Memory Networks for Anomaly Detection in Time Series," *Proceedings of the European Symposium on Artificial Neural Networks (ESANN)*, 2015.

[6] X. Zhang, Y. Sun, and P. Wang, "Anomaly Detection for Cloud-Based User Behavior Using Deep Learning," *IEEE Access*, vol. 10, pp. 57812–57824, 2022. DOI: 10.1109/ACCESS.2022.3172670

[7] T. Kim and J. Kim, "Privacy-Preserving Anomaly Detection for Federated Cloud Environments," *Future Generation Computer Systems*, vol. 143, pp. 322–334, 2023. DOI: 10.1016/j.future.2023.02.012

[8] He, Z., & Lee, R. B. (2021). *CloudShield: Real-time anomaly detection in the cloud.* ACM. https://doi.org/10.1145/3577923.3583639

[9] Nwachukwu, C., Durodola-Tunde, K., & Akwiwu-Uzoma, C. (2024). *AI-driven anomaly detection in cloud computing environments. International Journal of Science and Research Archive, 13*(2), 692–710. https://doi.org/10.30574/ijsra.2024.13.2.2184

[10] Van Ede, T., Khasuntsev, N., Steen, B., & Continella, A. (2022). *Detecting anomalous misconfigurations in AWS identity and access management policies.* In *Proceedings of the ACM Cloud Computing Security Workshop (CCSW '22).* https://doi.org/10.1145/3560810.3564264

[11] Hariharan, R. (2025). *AI-driven identity and access management in enterprise systems. International Journal of the Internet of Things*, 5(1), 62–94. https://doi.org/10.55640/ijiot-05-01-05

[12] Zhang, Z., Zhu, Z., Xu, C., Zhang, J., & Xu, S. (2024). *Towards accurate anomaly detection for cloud systems via graph-enhanced contrastive learning. Complex & Intelligent Systems, 11*(23). https://doi.org/10.1007/s40747-024-01659-x

1. [13] Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025, September). Climate-aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006
2. Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005
3. Tabassum, M., Rokibuzzaman, M., Islam, M. I., & Bristy, I. J. (2025, September). Data-driven financial analytics through MIS platforms in emerging economies. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 440–446. https://doi.org/10.36348/sjet.2025.v10i09.007
4. Tabassum, M., Islam, M. I., Bristy, I. J., & Rokibuzzaman, M. (2025, September). Blockchain and ERP-integrated MIS for transparent apparel & textile supply chains. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 447–456. https://doi.org/10.36348/sjet.2025.v10i09.008
5. Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025, September). IoT-driven predictive maintenance dashboards in industrial operations. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 457–466. https://doi.org/10.36348/sjet.2025.v10i09.009
6. Hasan, M. N., Karim, M. A., Joarder, M. M. I., & Zaman, M. T. (2025, September). IoT-integrated solar energy monitoring and bidirectional DC-DC converters for smart grids. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 467–475. https://doi.org/10.36348/sjet.2025.v10i09.010
7. Bormon, J. C., Saikat, M. H., Shohag, M., & Akter, E. (2025, September). Green and low-carbon construction materials for climate-adaptive civil structures. *Saudi Journal of Civil Engineering (SJCE), 9*(8), 219–226. https://doi.org/10.36348/sjce.2025.v09i08.002
8. Razaq, A., Rahman, M., Karim, M. A., & Hossain, M. T. (2025, September 26). Smart charging infrastructure for EVs using IoT-based load balancing. *Zenodo*. https://doi.org/10.5281/zenodo.17210639
9. Habiba, U., & Musarrat, R., (2025). Bridging IT and education: Developing smart platforms for student-centered English learning. *Zenodo*. https://doi.org/10.5281/zenodo.17193947
10. Alimozzaman, D. M. (2025). *Early prediction of Alzheimer's disease using explainable multi-modal AI.* Zenodo. https://doi.org/10.5281/zenodo.17210997
11. uz Zaman, M. T. Smart Energy Metering with IoT and GSM Integration for Power Loss Minimization. Preprints 2025, 2025091770. https://doi.org/10.20944/preprints202509.1770.v1
12. Hossain, M. T. (2025, October). *Sustainable garment production through Industry 4.0 automation.* ResearchGate. https://doi.org/10.13140/RG.2.2.20161.83041
13. Hasan, E. (2025). *Secure and scalable data management for digital transformation in finance and IT systems*. Zenodo. https://doi.org/10.5281/zenodo.17202282
14. Saikat, M. H. (2025). *Geo-Forensic Analysis of Levee and Slope Failures Using Machine Learning.* Preprints. https://doi.org/10.20944/preprints202509.1905.v1
15. Islam, M. I. (2025). *Cloud-Based MIS for Industrial Workflow Automation.* Preprints. https://doi.org/10.20944/preprints202509.1326.v1

16. Islam, M. I. (2025). *AI-powered MIS for risk detection in industrial engineering projects*. TechRxiv. https://doi.org/10.36227/techrxiv.175825736.65590627/v1
17. Akter, E. (2025, October 13). *Lean project management and multi-stakeholder optimization in civil engineering projects*. ResearchGate. https://doi.org/10.13140/RG.2.2.15777.47206
18. Musarrat, R. (2025). *Curriculum adaptation for inclusive classrooms: A sociological and pedagogical approach*. Zenodo. https://doi.org/10.5281/zenodo.17202455
19. Bormon, J. C. (2025, October 13). *Sustainable dredging and sediment management techniques for coastal and riverine infrastructure*. ResearchGate. https://doi.org/10.13140/RG.2.2.28131.00803
20. Bormon, J. C. (2025). AI-Assisted Structural Health Monitoring for Foundations and High-Rise Buildings. Preprints. https://doi.org/10.20944/preprints202509.1196.v1
21. Haque, S. (2025). *Effectiveness of managerial accounting in strategic decision making* [Preprint]. Preprints. https://doi.org/10.20944/preprints202509.2466.v1
22. Shoag, M. (2025). AI-Integrated Façade Inspection Systems for Urban Infrastructure Safety. Zenodo. https://doi.org/10.5281/zenodo.17101037
23. Shoag, M. Automated Defect Detection in High-Rise Façades Using AI and Drone-Based Inspection. Preprints 2025, 2025091064. https://doi.org/10.20944/preprints202509.1064.v1
24. Shoag, M. (2025). *Sustainable construction materials and techniques for crack prevention in mass concrete structures*. Available at SSRN: https://ssrn.com/abstract=5475306 or http://dx.doi.org/10.2139/ssrn.5475306
25. Joarder, M. M. I. (2025). *Disaster recovery and high-availability frameworks for hybrid cloud environments*. Zenodo. https://doi.org/10.5281/zenodo.17100446
26. Joarder, M. M. I. (2025). *Next-generation monitoring and automation: AI-enabled system administration for smart data centers*. TechRxiv. https://doi.org/10.36227/techrxiv.175825633.33380552/v1
27. Joarder, M. M. I. (2025). Energy-Efficient Data Center Virtualization: Leveraging AI and CloudOps for Sustainable Infrastructure. Zenodo. https://doi.org/10.5281/zenodo.17113371
28. Taimun, M. T. Y., Sharan, S. M. I., Azad, M. A., & Joarder, M. M. I. (2025). Smart maintenance and reliability engineering in manufacturing. *Saudi Journal of Engineering and Technology, 10*(4), 189–199.
29. Enam, M. M. R., Joarder, M. M. I., Taimun, M. T. Y., & Sharan, S. M. I. (2025). Framework for smart SCADA systems: Integrating cloud computing, IIoT, and cybersecurity for enhanced industrial automation. *Saudi Journal of Engineering and Technology, 10*(4), 152–158.
30. Azad, M. A., Taimun, M. T. Y., Sharan, S. M. I., & Joarder, M. M. I. (2025). Advanced lean manufacturing and automation for reshoring American industries. *Saudi Journal of Engineering and Technology, 10*(4), 169–178.
31. Sharan, S. M. I., Taimun, M. T. Y., Azad, M. A., & Joarder, M. M. I. (2025). Sustainable manufacturing and energy-efficient production systems. *Saudi Journal of Engineering and Technology, 10*(4), 179–188.
32. Farabi, S. A. (2025). *AI-augmented OTDR fault localization framework for resilient rural fiber networks in the United States*. arXiv. https://arxiv.org/abs/2506.03041
33. Farabi, S. A. (2025). *AI-driven predictive maintenance model for DWDM systems to enhance fiber network uptime in underserved U.S. regions*. Preprints. https://doi.org/10.20944/preprints202506.1152.v1
34. Farabi, S. A. (2025). *AI-powered design and resilience analysis of fiber optic networks in disaster-prone regions*. ResearchGate. https://doi.org/10.13140/RG.2.2.12096.65287
35. Sunny, S. R. (2025). *Lifecycle analysis of rocket components using digital twins and multiphysics simulation*. ResearchGate. https://doi.org/10.13140/RG.2.2.20134.23362
36. Sunny, S. R. (2025). *AI-driven defect prediction for aerospace composites using Industry 4.0 technologies*. Zenodo. https://doi.org/10.5281/zenodo.16044460
37. Sunny, S. R. (2025). *Edge-based predictive maintenance for subsonic wind tunnel systems using sensor analytics and machine learning*. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1
38. Sunny, S. R. (2025). *Digital twin framework for wind tunnel-based aeroelastic structure evaluation*. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1
39. Sunny, S. R. (2025). Real-time wind tunnel data reduction using machine learning and JR3 balance integration. *Saudi Journal of Engineering and Technology, 10*(9), 411–420. https://doi.org/10.36348/sjet.2025.v10i09.004
40. Sunny, S. R. (2025). AI-augmented aerodynamic optimization in subsonic wind tunnel testing for UAV prototypes. *Saudi Journal of Engineering and Technology, 10*(9), 402–410. https://doi.org/10.36348/sjet.2025.v10i09.003
41. Shaikat, M. F. B. (2025). *Pilot deployment of an AI-driven production intelligence platform in a textile assembly line*. TechRxiv. https://doi.org/10.36227/techrxiv.175203708.81014137/v1
42. Rabbi, M. S. (2025). *Extremum-seeking MPPT control for Z-source inverters in grid-connected solar PV systems*. Preprints. https://doi.org/10.20944/preprints202507.2258.v1
43. Rabbi, M. S. (2025). *Design of fire-resilient solar inverter systems for wildfire-prone U.S. regions*. Preprints. https://www.preprints.org/manuscript/202507.2505/v1
44. Rabbi, M. S. (2025). *Grid synchronization algorithms for intermittent renewable energy sources using AI control loops*. Preprints. https://www.preprints.org/manuscript/202507.2353/v1
45. Tonoy, A. A. R. (2025). *Condition monitoring in power transformers using IoT: A model for predictive maintenance*. Preprints. https://doi.org/10.20944/preprints202507.2379.v1
46. Tonoy, A. A. R. (2025). *Applications of semiconducting electrides in mechanical energy conversion and piezoelectric systems*. Preprints. https://doi.org/10.20944/preprints202507.2421.v1
47. Azad, M. A. (2025). *Lean automation strategies for reshoring U.S. apparel manufacturing: A sustainable approach*. Preprints. https://doi.org/10.20944/preprints202508.0024.v1
48. Azad, M. A. (2025). *Optimizing supply chain efficiency through lean Six Sigma: Case studies in textile and apparel manufacturing*. Preprints. https://doi.org/10.20944/preprints202508.0013.v1
49. Azad, M. A. (2025). *Sustainable manufacturing practices in the apparel industry: Integrating eco-friendly materials and processes*. TechRxiv. https://doi.org/10.36227/techrxiv.175459827.79551250/v1
50. Azad, M. A. (2025). *Leveraging supply chain analytics for real-time decision making in apparel manufacturing*. TechRxiv. https://doi.org/10.36227/techrxiv.175459831.14441929/v1
51. Azad, M. A. (2025). *Evaluating the role of lean manufacturing in reducing production costs and enhancing efficiency in textile mills*. TechRxiv. https://doi.org/10.36227/techrxiv.175459830.02641032/v1
52. Azad, M. A. (2025). *Impact of digital technologies on textile and apparel manufacturing: A case for U.S. reshoring*. TechRxiv. https://doi.org/10.36227/techrxiv.175459829.93863272/v1
53. Rayhan, F. (2025). *A hybrid deep learning model for wind and solar power forecasting in smart grids*. Preprints. https://doi.org/10.20944/preprints202508.0511.v1
54. Rayhan, F. (2025). *AI-powered condition monitoring for solar inverters using embedded edge devices*. Preprints. https://doi.org/10.20944/preprints202508.0474.v1
55. Rayhan, F. (2025). *AI-enabled energy forecasting and fault detection in off-grid solar networks for rural electrification*. TechRxiv. https://doi.org/10.36227/techrxiv.175623117.73185204/v1
56. Habiba, U., & Musarrat, R. (2025). Integrating digital tools into ESL pedagogy: A study on multimedia and student engagement. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 799–811. https://doi.org/10.5281/zenodo.17245996
57. Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT-based electric vehicle ecosystems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184
58. Hossain, M. T., Nabil, S. H., Rahman, M., & Razaq, A. (2025). Data analytics for IoT-driven EV battery health monitoring. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 903–913. https://doi.org/10.5281/zenodo.17246168
59. Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025). Digital twin technology for smart civil infrastructure and emergency preparedness. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 891–902. https://doi.org/10.5281/zenodo.17246150
60. Rahmatullah, R. (2025). Smart agriculture and Industry 4.0: Applying industrial engineering tools to improve U.S. agricultural productivity.

World Journal of Advanced Engineering Technology and Sciences, 17(1), 28–40. https://doi.org/10.30574/wjaets.2025.17.1.1377
61. Islam, R. (2025). *AI and big data for predictive analytics in pharmaceutical quality assurance.*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319
62. Rahmatullah, R. (2025). *Sustainable agriculture supply chains: Engineering management approaches for reducing post-harvest loss in the U.S. International Journal of Scientific Research and Engineering Development, 8*(5), 1187–1216. https://doi.org/10.5281/zenodo.17275907
63. Haque, S., Al Sany, S. M. A., & Rahman, M. (2025). *Circular economy in fashion: MIS-driven digital product passports for apparel traceability. International Journal of Scientific Research and Engineering Development, 8*(5), 1254–1262. https://doi.org/10.5281/zenodo.17276038
64. Al Sany, S. M. A., Haque, S., & Rahman, M. (2025). *Green apparel logistics: MIS-enabled carbon footprint reduction in fashion supply chains. International Journal of Scientific Research and Engineering Development, 8*(5), 1263–1272. https://doi.org/10.5281/zenodo.17276049
65. Bormon, J. C. (2025), Numerical Modeling of Foundation Settlement in High-Rise Structures Under Seismic Loading. Available at *SSRN*: https://ssrn.com/abstract=5472006 or http://dx.doi.org/10.2139/ssrn.5472006
66. Tabassum, M. (2025, October 6). *MIS-driven predictive analytics for global shipping and logistics optimization*. TechRxiv. https://doi.org/10.36227/techrxiv.175977232.23537711/v1
67. Tabassum, M. (2025, October 6). *Integrating MIS and compliance dashboards for international trade operations*. TechRxiv. https://doi.org/10.36227/techrxiv.175977233.37119831/v1
68. Zaman, M. T. U. (2025, October 6). *Predictive maintenance of electric vehicle components using IoT sensors. TechRxiv.* https://doi.org/10.36227/techrxiv.175978928.82250472/v1
69. Hossain, M. T. (2025, October 7). *Smart inventory and warehouse automation for fashion retail.* TechRxiv. https://doi.org/10.36227/techrxiv.175987210.04689809.v1
70. Karim, M. A. (2025, October 6). *AI-driven predictive maintenance for solar inverter systems*. TechRxiv. https://doi.org/10.36227/techrxiv.175977633.34528041.v1
71. Jahan Bristy, I. (2025, October 6). *Smart reservation and service management systems: Leveraging MIS for hotel efficiency*. TechRxiv. https://doi.org/10.36227/techrxiv.175979180.05153224.v1
72. Habiba, U. (2025, October 7). *Cross-cultural communication competence through technology-mediated TESOL.* TechRxiv. https://doi.org/10.36227/techrxiv.175985896.67358551.v1
73. Habiba, U. (2025, October 7). *AI-driven assessment in TESOL: Adaptive feedback for personalized learning*. TechRxiv. https://doi.org/10.36227/techrxiv.175987165.56867521.v1
74. Akhter, T. (2025, October 6). *Algorithmic internal controls for SMEs using MIS event logs*. TechRxiv. https://doi.org/10.36227/techrxiv.175978941.15848264.v1
75. Akhter, T. (2025, October 6). *MIS-enabled workforce analytics for service quality & retention*. TechRxiv. https://doi.org/10.36227/techrxiv.175978943.38544757.v1
76. Hasan, E. (2025, October 7). *Secure and scalable data management for digital transformation in finance and IT systems*. Zenodo. https://doi.org/10.5281/zenodo.17202282
77. Saikat, M. H., Shoag, M., Akter, E., Bormon, J. C. (October 06, 2025.) Seismic- and Climate-Resilient Infrastructure Design for Coastal and Urban Regions. *TechRxiv.* DOI: 10.36227/techrxiv.175979151.16743058/v1
78. Saikat, M. H. (October 06, 2025). AI-Powered Flood Risk Prediction and Mapping for Urban Resilience. *TechRxiv.* DOI: 10.36227/techrxiv.175979253.37807272/v1
79. Akter, E. (September 15, 2025). Sustainable Waste and Water Management Strategies for Urban Civil Infrastructure. Available at SSRN: https://ssrn.com/abstract=5490686 or http://dx.doi.org/10.2139/ssrn.5490686
80. Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025, October 6). *AI-enabled smart energy meters with DC-DC converter integration for electric vehicle charging systems.* TechRxiv. https://doi.org/10.36227/techrxiv.175978935.59813154/v1
81. Al Sany, S. M. A., Rahman, M., & Haque, S. (2025). *Sustainable garment production through Industry 4.0 automation. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 145–156. https://doi.org/10.30574/wjaets.2025.17.1.1387
82. Rahman, M., Haque, S., & Al Sany, S. M. A. (2025). *Federated learning for privacy-preserving apparel supply chain analytics. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386
83. Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). *Machine learning approaches for predictive maintenance in IoT devices. World Journal of Advanced Engineering Technology and Sciences, 17*(1), 157–170. https://doi.org/10.30574/wjaets.2025.17.1.1388
84. Akhter, T., Alimozzaman, D. M., Hasan, E., & Islam, R. (2025, October). *Explainable predictive analytics for healthcare decision support. International Journal of Sciences and Innovation Engineering, 2*(10), 921–938. https://doi.org/10.70849/IJSCI02102025105
85. Islam, M. S., Islam, M. I., Mozumder, A. Q., Khan, M. T. H., Das, N., & Mohammad, N. (2025). A Conceptual Framework for Sustainable AI-ERP Integration in Dark Factories: Synthesising TOE, TAM, and IS Success Models for Autonomous Industrial Environments. *Sustainability*, *17*(20), 9234. https://doi.org/10.3390/su17209234
86. Haque, S., Islam, S., Islam, M. I., Islam, S., Khan, R., Tarafder, T. R., & Mohammad, N. (2025). *Enhancing adaptive learning, communication, and therapeutic accessibility through the integration of artificial intelligence and data-driven personalization in digital health platforms for students with autism spectrum disorder. Journal of Posthumanism, 5*(8), 737–756. Transnational Press London.
87. Faruq, O., Islam, M. I., Islam, M. S., Tarafder, M. T. R., Rahman, M. M., Islam, M. S., & Mohammad, N. (2025). Re-imagining Digital Transformation in the United States: Harnessing Artificial Intelligence and Business Analytics to Drive IT Project Excellence in the Digital Innovation Landscape. *Journal of Posthumanism*, *5*(9), 333–354 . https://doi.org/10.63332/joph.v5i9.3326
88. Rahman, M.. (October 15, 2025) Integrating IoT and MIS for Last-Mile Connectivity in Residential Broadband Services. *TechRxiv.* **DOI: 10.36227/techrxiv.176054689.95468219/v1**
89. **Islam, R.** (2025, October 15). *Integration of IIoT and MIS for smart pharmaceutical manufacturing* . TechRxiv. https://doi.org/10.36227/techrxiv.176049811.10002169
90. Hasan, E. (2025). Big Data-Driven Business Process Optimization: Enhancing Decision-Making Through Predictive Analytics. TechRxiv. October 07, 2025. **10.36227/techrxiv.175987736.61988942/v1**
91. **Rahman, M.** (2025, October 15). *IoT-enabled smart charging systems for electric vehicles* [Preprint]. TechRxiv. https://doi.org/10.36227/techrxiv.176049766.60280824
92. Alam, M. S. (2025, October 21). *AI-driven sustainable manufacturing for resource optimization*. *TechRxiv.* https://doi.org/10.36227/techrxiv.176107759.92503137/v1
93. Alam, M. S. (2025, October 21). *Data-driven production scheduling for high-mix manufacturing environments*. *TechRxiv.* https://doi.org/10.36227/techrxiv.176107775.59550104/v1
94. Ria, S. J. (2025, October 21). *Environmental impact assessment of transportation infrastructure in rural Bangladesh*. *TechRxiv.* https://doi.org/10.36227/techrxiv.176107782.23912238/v1
95. R Musarrat and U Habiba, Immersive Technologies in ESL Classrooms: Virtual and Augmented Reality for Language Fluency (September 22, 2025). Available at SSRN: https://ssrn.com/abstract=5536098 or http://dx.doi.org/10.2139/ssrn.5536098
96. Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025), "AI-Enabled Structural and Façade Health Monitoring for Resilient Cities", *Int. J. Sci. Inno. Eng.*, vol. 2, no. 10, pp. 1035–1051, Oct. 2025, doi: 10.70849/IJSCI02102025116
97. Haque, S., Al Sany (Oct. 2025), "Impact of Consumer Behavior Analytics on Telecom Sales Strategy", *Int. J. Sci. Inno. Eng.*, vol. 2, no. 10, pp. 998–1018, doi: 10.70849/IJSCI02102025114.
98. Sharan, S. M. I (Oct. 2025)., "Integrating Human-Centered Design with Agile Methodologies in Product Lifecycle Management", *Int. J. Sci. Inno. Eng.*, vol. 2, no. 10, pp. 1019–1034, doi: 10.70849/IJSCI02102025115.
99. Alimozzaman, D. M. (2025). Explainable AI for early detection and classification of childhood leukemia using multi-modal medical data.

World Journal of Advanced Engineering Technology and Sciences, 17(2), 48–62. https://doi.org/10.30574/wjaets.2025.17.2.1442

100. Alimozzaman, D. M., Akhter, T., Islam, R., & Hasan, E. (2025). Generative AI for synthetic medical imaging to address data scarcity. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 544–558. https://doi.org/10.30574/wjaets.2025.17.1.1415
101. Zaidi, S. K. A. (2025). Intelligent automation and control systems for electric vertical take-off and landing (eVTOL) drones. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 63–75. https://doi.org/10.30574/wjaets.2025.17.2.1457
102. Islam, K. S. A. (2025). Implementation of safety-integrated SCADA systems for process hazard control in power generation plants. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2321–2331. Zenodo. https://doi.org/10.5281/zenodo.17536369
103. Islam, K. S. A. (2025). Transformer protection and fault detection through relay automation and machine learning. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2308–2320. Zenodo. https://doi.org/10.5281/zenodo.17536362
104. Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2298–2307. Zenodo. https://doi.org/10.5281/zenodo.17536343
105. Al Sany, S. M. A. (2025). The role of data analytics in optimizing budget allocation and financial efficiency in startups. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2287–2297. Zenodo. https://doi.org/10.5281/zenodo.17536325
106. Zaman, S. (2025). Vulnerability management and automated incident response in corporate networks. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2275–2286. Zenodo. https://doi.org/10.5281/zenodo.17536305
107. Ria, S. J. (2025, October 7). *Sustainable construction materials for rural development projects.* SSRN. https://doi.org/10.2139/ssrn.5575390
108. Razaq, A. (2025, October 15). *Design and implementation of renewable energy integration into smart grids.* TechRxiv. https://doi.org/10.36227/techrxiv.176049834.44797235/v1
109. Musarrat R. (2025). AI-Driven Smart Housekeeping and Service Allocation Systems: Enhancing Hotel Operations Through MIS Integration. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 898–910). Zenodo. https://doi.org/10.5281/zenodo.17769627
110. Hossain, M. T. (2025). AI-Augmented Sensor Trace Analysis for Defect Localization in Apparel Production Systems Using OTDR-Inspired Methodology. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1029–1040). Zenodo. https://doi.org/10.5281/zenodo.17769857
111. Rahman M. (2025). Design and Implementation of a Data-Driven Financial Risk Management System for U.S. SMEs Using Federated Learning and Privacy-Preserving AI Techniques. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1041–1052). Zenodo. https://doi.org/10.5281/zenodo.17769869
112. Alam, M. S. (2025). Real-Time Predictive Analytics for Factory Bottleneck Detection Using Edge-Based IIoT Sensors and Machine Learning. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1053–1064). Zenodo. https://doi.org/10.5281/zenodo.17769890
113. Habiba, U., & Musarrat, R. (2025). Student-centered pedagogy in ESL: Shifting from teacher-led to learner-led classrooms. *International Journal of Science and Innovation Engineering*, 2(11), 1018–1036. https://doi.org/10.70849/IJSCI02112025110
114. Zaidi, S. K. A. (2025). Smart sensor integration for energy-efficient avionics maintenance operations. *International Journal of Science and Innovation Engineering*, 2(11), 243–261. https://doi.org/10.70849/IJSCI02112025026
115. Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering*, 2(11), 220–242. https://doi.org/10.70849/IJSCI02112025025
116. Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. *World Journal of Advanced Engineering Technology and Sciences*, 17(02), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458
117. Saeed, H. N. (2025). Hybrid perovskite–CIGS solar cells with machine learning-driven performance prediction. *International Journal of Science and Innovation Engineering*, 2(11), 262–280. https://doi.org/10.70849/IJSCI02112025027
118. Akter, E. (2025). Community-based disaster risk reduction through infrastructure planning. *International Journal of Science and Innovation Engineering*, 2(11), 1104–1124. https://doi.org/10.70849/IJSCI02112025117
119. Akter, E. (2025). Green project management framework for infrastructure development. *International Journal of Science and Innovation Engineering*, 2(11), 1125–1144. https://doi.org/10.70849/IJSCI02112025118
120. Shoag, M. (2025). Integration of lean construction and digital tools for façade project efficiency. *International Journal of Science and Innovation Engineering*, 2(11), 1145–1164. https://doi.org/10.70849/IJSCI02112025119
121. Akter, E. (2025). Structural Analysis of Low-Cost Bridges Using Sustainable Reinforcement Materials. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 911–921). Zenodo. https://doi.org/10.5281/zenodo.17769637
122. Razaq, A. (2025). Optimization of power distribution networks using smart grid technology. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 129–146. https://doi.org/10.30574/wjaets.2025.17.3.1490
123. Zaman, M. T. (2025). Enhancing grid resilience through DMR trunking communication systems. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 197–212. https://doi.org/10.30574/wjaets.2025.17.3.1551
124. Nabil, S. H. (2025). Enhancing wind and solar power forecasting in smart grids using a hybrid CNN-LSTM model for improved grid stability and renewable energy integration. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 213–226. https://doi.org/10.30574/wjaets.2025.17.3.155
125. Nahar, S. (2025). Optimizing HR management in smart pharmaceutical manufacturing through IIoT and MIS integration. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 240–252. https://doi.org/10.30574/wjaets.2025.17.3.1554
126. Islam, S. (2025). IPSC-derived cardiac organoids: Modeling heart disease mechanism and advancing regenerative therapies. *World Journal of Advanced Engineering Technology and Sciences*, 17(03), 227–239. https://doi.org/10.30574/wjaets.2025.17.3.1553

