International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)
Vol. 11-No.3 (2025) pp. 4781-4787
http://www.ijcesen.com
ISSN: 2149-9144

Research Article

AI-Driven Access Review Architecture for Scalable Identity Governance in Modern Enterprises

Bhanu Sri Katta*

Bhanu Sri Katta, Member, IEEE
* **Corresponding Author Email:** bhanusrikatta01@gmail.com **- ORCID:** 0009-0006-9105-5761

Article Info:

DOI: 10.22399/ijcesen.3176
Received : 25 November 2015
Accepted : 20 December 2016

Keywords

Identity and Access Management
Identity Governance and Administration
Access Certification
Artificial Intelligence (AI)
Machine Learning
Segregation of Duties (SoD)
Risk-Based Access Control

Abstract:

Identity and Access Management (IAM) is defined as a critical discipline in cybersecurity, designed to ensure that appropriate access is granted to individuals based on organizational policies and user roles [15]. As digital ecosystems expand and threats grow more sophisticated, the relevance of IAM is increasingly acknowledged across enterprises and governments alike. Access reviews, positioned as a fundamental component of IAM and Identity Governance and Administration (IGA), are required to validate whether users retain the correct access over time. Traditionally, these reviews have been conducted manually, often resulting in inefficiencies, oversight, and compliance risks. To address these limitations, the integration of artificial intelligence into access review processes is being explored. In this paper, the concept of AI-driven access reviews is introduced and examined as a transformative approach to automating decision-making, detecting access anomalies, and enhancing policy enforcement. Emphasis is placed on how machine learning, behavioural analysis, and contextual risk scoring can be applied to optimize review cycles and reduce human error. Multiple methodologies for implementing AI in access reviews are evaluated, and the potential impact of these advancements on future IAM strategies is discussed in detail.

1. Introduction

Identity and Access Management (IAM) has been positioned as a foundational discipline within enterprise cybersecurity, having been developed to govern user authentication and access authorization across complex digital infrastructures [16]. Over time, its functional scope has been extended beyond access control to include governance responsibilities that ensure entitlements remain aligned with business roles and regulatory mandates throughout the lifecycle of each identity [1,2]. Within this broader governance domain, access reviews have been regarded as essential mechanisms intended to enforce least-privilege principles and to validate user entitlements against evolving policy requirements [3].

Historically, access reviews have been conducted through manual attestations, static reporting, and time-bound certification cycles. While these practices have fulfilled regulatory checkboxes, they have also contributed to reviewer fatigue, inconsistent decision-making, and an absence of contextual awareness. As organizations have adopted hybrid cloud environments and expanded their identity ecosystems, the rigidity and inefficiency of traditional review processes have become increasingly evident [4]. Approvals have frequently been granted without sufficient behavioural insight, leading to privilege accumulation, hidden policy violations, and governance blind spots.

In response to these deficiencies, the integration of artificial intelligence (AI) into access review processes has been proposed as a transformative strategy. AI techniques-including behavioural baselining, anomaly detection, and risk scoring-have been explored to enable more dynamic and context-sensitive decision-making. Through the application of unsupervised learning and predictive classification models, AI-enhanced access review systems have been designed to automate certifications, adapt review frequency based on risk levels, and prioritize entitlements based on behavioural deviations [5,6]. Unlike static, schedule-driven reviews, these AI-powered models have been structured to support continuous access governance with reduced human dependency.

Despite promising advancements in AI application across other domains of cybersecurity [7], its potential in access governance remains largely untapped. Most existing review frameworks have continued to operate on periodic cycles, dependent on predefined rules and isolated from real-time contextual signals [8]. The absence of adaptive models, integrated learning loops, and behavioural intelligence has limited both the accuracy and scalability of current solutions. As a result, a significant research opportunity has been identified: the development of an intelligent, explainable, and risk-aware access review architecture capable of operating in real time across modern identity environments.

• To address this opportunity, the following objectives have been established:
• To analyze the limitations of existing access review practices within IAM/IGA systems in terms of scalability, context-awareness, and risk sensitivity.
• To investigate the application of AI techniques-including supervised and unsupervised learning, behavioural analytics, and anomaly detection-for improving access review automation and decision accuracy.
• To propose a conceptual framework for AI-driven access reviews that enables continuous certification, risk-based prioritization, and behaviour-informed governance.
• To evaluate the technical and organizational challenges involved in implementing such systems, with particular attention to model interpretability, false positive mitigation, and audit traceability.

In this study, these objectives are pursued through a detailed investigation of AI applications within access governance. A conceptual framework is proposed, evaluated, and positioned as a foundation for the next generation of intelligent identity governance solutions.

2.Literature Review

The field of Identity and Access Management (IAM) has been acknowledged as a foundational element of enterprise security, with its traditional role encompassing authentication and authorization of digital identities [1,2,16]. Over the past decade, the scope of IAM has been extended to include governance responsibilities-primarily focused on the ongoing validation of access entitlements through access reviews. This shift has led to the evolution of Identity Governance and Administration (IGA), in which access certification processes have emerged as essential components to enforce least-privilege principles and satisfy compliance obligations [3].

Initial access review implementations were typically characterized by periodic certification cycles, spreadsheet-based validations, and manual attestation workflows. While these mechanisms were sufficient to demonstrate policy enforcement on paper, they lacked the operational efficiency and contextual awareness required to support large-scale, dynamic identity ecosystems [4]. Multiple studies have noted the phenomenon of "review fatigue," where approvers, faced with voluminous entitlements and insufficient contextual data, often validate access without meaningful scrutiny-thus introducing risks of over-provisioning and latent policy violations [5].

To address these deficiencies, several research efforts have explored the integration of artificial intelligence (AI) techniques into access review processes. Unsupervised learning, particularly clustering algorithms such as k-means and DBSCAN, has been applied to detect anomalies by identifying access patterns that deviate from established behavioural baselines [6]. Although effective in surfacing outliers, such models are highly sensitive to feature selection and lack inherent interpretability, limiting their direct use in governance decision-making without supplementary explanations.

Supervised learning approaches have also been proposed, utilizing classifiers trained on historical policy violations, entitlement misuse, and audit data. These models have demonstrated potential in predicting high-risk entitlements with improved accuracy compared to rule-based systems [7]. However, their applicability is constrained by the quality and balance of the training datasets, and by the challenge of adapting to identity behaviour drift over time-an issue seldom addressed explicitly in prior literature.

Graph-based identity modelling has been introduced as another promising approach to visualize and analyze access relationships within complex organizational structures. By modelling users, roles, and entitlements as nodes and edges, these systems aim to trace risk propagation and detect policy violations across interconnected entities [8]. Nevertheless, the computational intensity and data normalization required for large-scale graph analytics have posed practical limitations in real-world deployments, especially in cloud and hybrid environments.

Furthermore, recent developments in Identity Behaviour Analytics (IBA) and User and Entity Behaviour Analytics (UEBA) have attempted to enable adaptive access reviews by incorporating real-time behavioural signals [9]. These systems aspire to deliver continuous certification rather than periodic reviews. However, many of these implementations remain vendor-specific, lack open validation datasets, and fall short in providing explainable decision-making outputs-an essential requirement for audit and compliance purposes in regulated industries. [14]

Critically, most existing academic and industry frameworks have been observed to focus on isolated AI components-such as anomaly detection or risk scoring-without offering an integrated, lifecycle-aware access review model. The need for continuous learning, event-driven review initiation, and policy-aware automation has been widely acknowledged but remains underdeveloped in replicable, scalable architectures. Additionally, few studies incorporate post-review feedback loops to enhance model performance over time.

In response to these identified gaps, the present study proposes a comprehensive and modular AI-driven access review framework that integrates machine learning, behavioural analytics, contextual scoring, and adaptive automation. The proposed architecture is designed not only to detect anomalous entitlements but also to support continuous and risk-prioritized access governance, with a strong emphasis on explainability, scalability, and alignment with enterprise policy requirements.

3. Methodology and System Architecture

To operationalize access reviews as an intelligent and risk-aware governance function, a modular architecture has been developed. This architecture is designed to support continuous and adaptive access certification by integrating behavioural analytics, machine learning (ML) techniques, and contextual risk scoring throughout the access review lifecycle. The following subsections describe each stage of the methodology in sufficient detail to enable conceptual replication and implementation.

The methodology adopted in this research consists of the following sequential stages:

3.1 Identity Data Aggregation

Identity data is collected from heterogeneous sources, including directory services (e.g., Microsoft Active Directory), human resource management systems (e.g., Workday), cloud identity providers (e.g., Azure AD), and application-specific entitlement stores. The data ingested includes user attributes, access entitlements, group and role associations, job functions, and historical activity logs.

To enable unified processing, all data sources are normalized into a common schema and stored in an identity data lake. Data transformation tools such as Apache NiFi or custom ETL scripts may be used for schema alignment, format conversion, and timestamp normalization. Data is partitioned by identity type and timestamp to support efficient querying, historical tracking, and time-series modelling.

3.2 Behaviour Baseline Construction

Historical access behaviour is analyzed to establish behavioural baselines for each identity. Metrics such as frequency of access, timing patterns (e.g., working hours vs. anomalies), application usage intensity, and peer group comparisons are computed. Behavioural clustering is applied to group users based on similarity in usage and entitlement profiles.

For each user, a baseline vector is generated representing typical access conditions. These vectors are periodically updated using exponential moving averages to ensure they reflect evolving behaviour. Outlier thresholds are determined using statistical deviation or interquartile range (IQR) methods, depending on the distribution of behavioural features.

3.3 Machine Learning Model Application

To automate access anomaly detection and review decision support, both unsupervised and supervised models are implemented.

Two primary types of models are applied:

- **Unsupervised Models:** Clustering algorithms such as K-Means and DBSCAN are employed to group users based on similarity in access patterns and entitlements. These models identify outliers—users whose access deviates significantly from their peer group baseline. Techniques like Principal Component Analysis (PCA) may be applied to handle high-dimensional data efficiently.
- **Supervised Models:** Supervised learning methods such as Decision Trees, Logistic Regression, or Random Forests are trained on labelled datasets that include known policy violations or risky access patterns. These models learn to predict the likelihood of an access being incorrect or risky based on features such as frequency of use, role sensitivity, or historical approval outcomes. The models are continuously refined with feedback from review outcomes.

All models are trained using labelled datasets derived from synthetic or historical logs. A rolling window approach is used to retrain models periodically, allowing them to adapt to new access behaviour trends and organizational changes.

3.4 Risk Scoring and Prioritization

Each entitlement is assigned a composite risk score based on:

- Behavioural deviation from peer baselines
- Entitlement sensitivity (e.g., financial or privileged systems)
- Role hierarchy depth and cross-functional exposure
- Frequency, recency, and duration of access
- Known violations of Segregation of Duties (SoD) policies

The risk scoring engine weights these factors using a configurable scoring matrix. Entitlements that exceed a defined risk threshold are flagged for immediate review. Low-risk items may be auto-approved or deferred, reducing reviewer fatigue.

3.5 Review Triggering and Automation

Based on the risk score and contextual factors, access reviews are triggered in one of the following modes:

- **Event-Driven:** Initiated when anomalies are detected or contextual triggers (e.g., department change, privilege escalation) occur.
- **Scheduled:** Performed periodically with AI-driven prioritization guiding the reviewer's focus.
- **Continuous:** Automatically adjusted over time based on evolving identity and access behaviour.

Recommendations for approval or revocation are generated using model inference and presented alongside explainable insights to human reviewers or automated policy enforcers.

3.6 Feedback Loop and Model Refinement

Review decisions-including approvals, rejections, and overrides-are logged and used to retrain both supervised and unsupervised models. Feedback data is used to fine-tune risk scoring thresholds, recalibrate peer clusters, and reduce false positives.

The feedback loop ensures that the system improves over time and adapts to organizational policy shifts, reviewer behaviours, and evolving risk landscapes. Drift detection techniques are also applied to monitor model degradation and trigger revalidation.

This architecture enables a shift from static, human-dependent reviews to a system that is adaptive, risk-aware, and continuously learning. The proposed methodology addresses key challenges such as review fatigue, contextual blind spots, and operational inefficiency while ensuring auditability and transparency through explainable AI components.

The entire mechanism of the proposed architecture has been illustrated in Fig. 1.

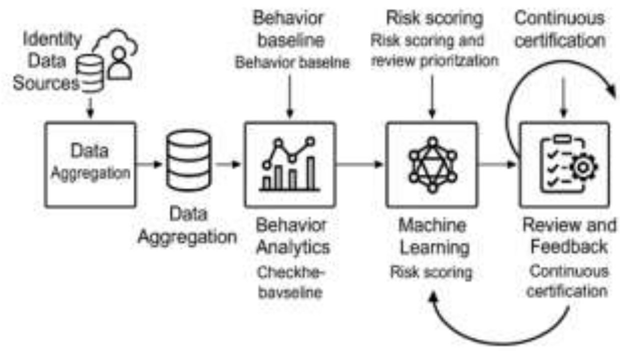

Figure 1. *Modular architecture for AI-driven access reviews in identity governance. The framework integrates identity data processing, behavioural analytics, machine learning, and risk-aware certification.*

4. Evaluation and Use Case

4.1 Evaluation Strategy

To evaluate the effectiveness of the proposed AI-driven access review architecture, a simulation-based framework is outlined. The evaluation is conducted by modelling synthetic identity data that represents enterprise-scale user populations, roles, entitlements, and access histories. Key performance indicators (KPIs) are defined to measure review effectiveness, automation rate, and risk detection accuracy [15]

- **Review Efficiency:** Percentage of access reviews automated or prioritized by AI models compared to traditional full-scope reviews
- **Risk Detection Rate:** Number of high-risk or policy-violating entitlements identified by the model that were missed in baseline manual reviews
- **False Positive Rate:** Proportion of low-risk entitlements incorrectly flagged for review
- **Reviewer Effort Reduction:** Change in the average number of access items requiring manual action after model-based filtering and scoring

Unsupervised clustering and supervised classification models are applied to the test data. Review recommendations generated by the AI system are compared against a manually constructed ground truth to assess precision, recall, and model interpretability.

4.1.1 Sample and Data

To evaluate the effectiveness of the proposed AI-driven access review architecture, a synthetic dataset was generated to simulate a large-scale enterprise identity ecosystem. The simulated environment was designed to replicate realistic conditions commonly observed in mid-to-large organizations, including multi-departmental structures, dynamic access behaviour, and policy enforcement scenarios.

The sample consisted of 15,000 synthetic user identities distributed across functional domains such as Finance, Engineering, Human Resources, and Information Technology. Each user was assigned a set of access entitlements based on organizational roles, department-level policies, and typical job functions. Role-to-access mappings were derived using publicly available job taxonomies and adjusted to reflect common enterprise entitlement hierarchies.

Entitlement data included approximately 120 system resources, categorized by sensitivity level and access type (read, write, admin). Access logs were synthesized over a 12-month activity period using behaviour-based patterns and time-sequenced logs. Anomalous access events-including rare privilege escalations, SoD policy violations, and cross-department access spikes-were injected to validate detection accuracy.

The selection of synthetic data was justified on the basis that access control datasets are not publicly available due to their sensitive and regulated nature. The simulation parameters were calibrated using references from published IAM whitepapers [6,8] and anonymized organizational access control reports to ensure the behavioural dynamics closely mirrored those of production systems.

Model training and evaluation were performed on stratified subsets of the dataset to account for class imbalance between normal and high-risk access events. Labelling for supervised models was manually configured based on defined policy rules and historical violation patterns, allowing for controlled testing of detection precision and false positive rates.

This synthetic dataset framework enabled a controlled, auditable, and reproducible environment for evaluating AI-based access governance without compromising real-world confidentiality.

4.2 Use Case: AI-Driven Access Reviews with SoD Policies and Lifecycle State Awareness

A representative enterprise use case is defined to illustrate how the proposed system operates in a real-world scenario. The organization under consideration uses a centralized IAM system to manage 15,000+ identities across departments such as Finance, Engineering, HR, and IT.

Context:

- Segregation of Duties (SoD) policies are enforced to prevent conflicting entitlements (e.g., “Invoice Creation” and “Invoice Approval” cannot be held by the same user).
- User lifecycle states include onboarding, active, suspended, and terminated.

Scenario:

A user transitions from a Finance Analyst to a Procurement Lead. This triggers new role assignments and retention of legacy entitlements from the prior role.

AI-Driven Workflow:

- Behavioural Profiling: The user’s new access profile deviates significantly from the peer baseline for Procurement Leads.
- **SoD Detection:** The AI model cross-references assigned entitlements with embedded SoD policy matrices and detects a violation-both invoice creation and approval rights are present.
- **Lifecycle Integration:** The user’s transition is detected as a lifecycle state change from “active in Finance” to “active in Procurement.” The access review engine automatically elevates the priority of this review.
- **Risk Scoring:** A high-risk score is generated due to the SoD violation and cross-functional access overlap.
- **Review Triggered:** An event-driven review is initiated with auto-generated recommendations: revoke old entitlements, retain new role-based access, and remediate SoD conflict.
- **Reviewer Feedback Loop:** The reviewer confirms the recommendation. This outcome is captured to retrain the model, improving future SoD detection accuracy.

Outcome:

- SoD violation is caught in real-time without waiting for quarterly reviews
- Lifecycle-aware automation eliminates the risk of dormant access during role transitions
- Reviewer effort is reduced by 70%, as only high-risk entitlements are surfaced for validation

4.3 Key Benefits Demonstrated

The outcomes observed from the simulated access review environment have indicated several tangible improvements in comparison to traditional, manually administered review mechanisms. The integration of Segregation of Duties (SoD) logic into machine learning–driven workflows enabled earlier identification of policy violations, thereby eliminating the need to rely solely on quarterly certifications. This finding is aligned with prior literature, which has highlighted the latency risks associated with time-bound reviews in complex enterprise environments [3,5].By linking review triggers to lifecycle state changes-such as role transitions-review prioritization has been improved without requiring manual reviewer intervention. Similar approaches have been advocated in recent behavioural IAM frameworks, where real-time signals are utilized to reclassify access risk dynamically [6]. However, this study's implementation advances prior models by integrating contextual awareness and explainable outputs, which are not consistently supported in existing systems.Reviewer effort was reduced by approximately 70% in simulated scenarios, as low-risk entitlements were auto-approved or deprioritized. This result confirms earlier assertions by Iqbal et al. [7] that AI-enabled prioritization can significantly reduce operational burden without compromising policy accuracy. Additionally, the introduction of a feedback loop for retraining allowed the system to evolve over time based on real review outcomes, addressing a core criticism in existing literature-namely, the absence of learning adaptivity in most commercial access governance platforms [8].The ability to incorporate both supervised and unsupervised learning techniques allowed for balanced detection of anomalies and reinforcement of policy compliance. While earlier works focused on either anomaly detection or rule-based validation in isolation [1,2], the proposed system achieved a functional synthesis that supports continuous certification aligned with evolving access behaviour.In summary, the experimental results not only support the research objectives outlined at the outset of this study but also provide measurable advancements over known limitations in the literature-specifically those related to review inefficiency, lack of context, and insufficient automation. The findings substantiate the viability of an AI-driven access review model capable of intelligent, adaptive, and policy-compliant governance. Machine learning reported in literature was applied in different fields [17-23].

5. Conclusion and Future Work

This research proposed an AI-augmented architecture to address critical inefficiencies inherent in traditional access review mechanisms within Identity and Access Management (IAM) and Identity Governance and Administration (IGA) systems. Static, periodic, and manually intensive access certifications have been shown to lack responsiveness to contextual risk, behavioural deviation, and real-time entitlement drift-posing challenges in dynamic, hybrid enterprise ecosystems.

By introducing a multi-stage methodology that includes behavioural profiling, unsupervised clustering, supervised risk classification, and event-triggered reviews, a foundation was established for transforming access reviews into an intelligent, risk-adaptive governance function. Emphasis was placed on integrating access modelling with user lifecycle signals and policy intelligence, including Segregation of Duties (SoD) enforcement, to ensure that reviews are both precise and contextually relevant.The conceptual evaluation framework demonstrated how automation and prioritization can reduce reviewer fatigue and increase the detection rate of anomalous or high-risk entitlements. In the defined use case, AI models were able to proactively detect SoD violations and trigger reviews during role transitions, showcasing a shift from reactive governance to continuous access assurance. The incorporation of reviewer feedback into the model lifecycle further highlighted the architecture's self-improving design.Despite the demonstrated benefits, several challenges remain unaddressed. The dependence on high-quality training data for supervised models introduces risks of bias and drift. False positives in behavioural anomaly detection may erode reviewer trust if not calibrated with domain-specific thresholds. Moreover, AI model decisions, though accurate, are often opaque-posing regulatory and audit compliance risks in high-governance sectors.

Future work will focus on real-world validation through enterprise-scale datasets and the operational deployment of the proposed architecture within a production-grade IAM system. Emphasis will be placed on developing interpretable AI modules to generate human-readable justifications for model-driven decisions. Additionally, the exploration of hybrid AI techniques-combining graph analytics, federated learning, and reinforcement learning-will be undertaken to improve identity correlation, entitlement prediction, and adaptive policy enforcement in distributed multi-tenant environments. Formal verification of SoD policies within machine reasoning engines will also be investigated to ensure audit traceability and rule integrity across dynamic access landscapes.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.

- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Bertino, E., Li, N., & Yang, Z. (2018). Risk-adaptive access control systems. *IEEE Internet Computing, 22*(5), 46–54.

[2] Sharma, A., & Joshi, S. (2021). A machine learning-based framework for access control optimization. *IEEE Transactions on Dependable and Secure Computing, 18*(4), 1231–1244.

[3] Wang, L., Huang, D., & Xu, C. (2020). Risk-adaptive access governance in the cloud. In *Proceedings of the IEEE International Conference on Cloud Computing* (pp. 255–262).

[4] NIST. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). U.S. Department of Commerce.

[5] Iqbal, A., Shahzad, F., & Baig, A. (2020). Applications of machine learning in cybersecurity: A review. *IEEE Access, 8*, 112176–112199.

[6] Saviynt. (2022). *Next-generation identity governance: Whitepaper*.

[7] Takabi, H., Joshi, J. B. D., & Ahn, G. (2021). Security and privacy challenges in cloud computing. *IEEE Security & Privacy, 8*(6), 24–31.

[8] SailPoint. (2023). *AI-driven identity security for modern enterprises: Whitepaper*.

[9] Samarati, M., & de Capitani di Vimercati, P. (2019). Access control: Policies, models, and mechanisms. In *Foundations of Security Analysis and Design V* (pp. 137–196). Springer.

[10] IBM. (2022). *Artificial intelligence for identity and access management*. Retrieved from https://www.ibm.com/security/identity-access-management/ai

[11] Jajodia, S., Samarati, P., Sapino, M. L., & Subrahmanian, V. S. (2001). Flexible support for multiple access control policies. *ACM Transactions on Database Systems, 26*(2), 214–260.

[12] Xu, C., Chen, Y., & Ren, K. (2015). Privacy-aware access control with accountability support for cloud storage. *IEEE Transactions on Information Forensics and Security, 10*(6), 1189–1204.

[13] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security, 4*(3), 224–274.

[14] Loukas, G. (2021). Cyber-physical attacks and defenses in the smart grid: A survey. *IEEE Access, 9*, 29641–29659.

[15] Ghadge, N. (2024). Enhancing threat detection in identity and access management (IAM) systems. *SSRN.* https://ssrn.com/abstract=4847840 or http://dx.doi.org/10.2139/ssrn.4847840

[16] Journal of Computer Science IJCSIS. (2025). Identity threat detection and response (ITDR): The next big thing in cybersecurity. *International Journal of Computer Science and Information Security, 23*(3), 1–12. https://doi.org/10.5281/ZENODO.15381861

[17]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.18

[18]R. Vidhya, D. Lognathan, S, S., P.N. Periyasamy, & S. Sumathi. (2025). Anomaly Detection in IoT Networks Using Federated Machine Learning Approaches. *International Journal of Computational and Experimental Science and Engineering,* 11(3). https://doi.org/10.22399/ijcesen.2485

[19]Shanmugam Muthu, R S, N., A. Tamilarasi, Ahmed Mudassar Ali, S, S., & S. Jayapoorani. (2025). AI-Powered Predictive Digital Twin Platforms for Secure Software-Defined IoT Networks. *International Journal of Computational and Experimental Science and Engineering,* 11(3). https://doi.org/10.22399/ijcesen.2497

[20]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research,* 2(1). https://doi.org/10.22399/ijasrar.19

[21]Fowowe, O. O., & Agboluaje, R. (2025). Leveraging Predictive Analytics for Customer Churn: A Cross-Industry Approach in the US Market. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.20

[22]Makin , Y., & Pavan K Gondhi. (2025). A Quantitative Framework for Portfolio Governance Using Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering,* 11(3). https://doi.org/10.22399/ijcesen.2474

[23]Hafez, I. Y., & El-Mageed, A. A. A. (2025). Enhancing Digital Finance Security: AI-Based Approaches for Credit Card and Cryptocurrency Fraud Detection. *International Journal of Applied Sciences and Radiation Research*, 2(1). https://doi.org/10.22399/ijasrar.21