International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

AI-Enabled Machine Learning Solutions for Cybersecurity and Web Analytics in Enterprise Healthcare Systems with SAP

Vinícius Gabriel Lopes

Independent Researcher, Brazil

ABSTRAC: The increasing digitization of enterprise healthcare systems has heightened the need for advanced cybersecurity and intelligent web analytics to protect sensitive data and ensure operational resilience. This study presents an AI-enabled machine learning framework designed to enhance cybersecurity and web analytics in enterprise healthcare environments using SAP platforms. The proposed approach leverages big data analytics and machine learning models to detect cyber threats, identify anomalies, and analyze web traffic patterns in real time. By integrating AI-driven security mechanisms with SAP-based enterprise systems, the framework enables proactive threat detection, risk mitigation, and improved system visibility. Privacy-aware controls, access management, and data governance mechanisms are incorporated to safeguard patient information and maintain regulatory compliance. Experimental analysis demonstrates improved detection accuracy, scalability, and performance, making the proposed solution suitable for large-scale, cloud-enabled healthcare enterprises.

KEYWORDS: AI, Machine Learning, Cybersecurity, Web Analytics, Enterprise Healthcare Systems, Big Data, SAP.

I. INTRODUCTION

In the digital age, organizations from every sector are increasingly dependent on interconnected computing systems, cloud-based services, mobile infrastructures, and Internet-enabled devices. While these technologies facilitate innovation and operational agility, they also expose enterprises to a broad array of cyber threats. Attackers exploit vulnerabilities in networks, applications, and human behavior, often operating under the radar of traditional security mechanisms. Conventional defense methods—such as static rule sets, signature-based intrusion detection systems, and manual log reviews—struggle to keep pace with evolving attack patterns that are dynamic, polymorphic, and often stealthy.

Recognizing these limitations, researchers and practitioners have turned to the fields of artificial intelligence (AI) and machine learning (ML) to develop automated, adaptive, and intelligent threat detection systems. These systems aspire to end-to-end visibility across organizational environments, enabling real-time identification of anomalous activity and proactive threat response. AI and ML bring the ability to process large volumes of telemetry data, learn intricate patterns of legitimate and malicious behavior, and detect subtle deviations indicative of security incidents.

End-to-end threat detection refers to the integration of monitoring, analysis, and response across the entire digital estate. This includes endpoints (desktops, servers, mobile devices), network traffic, cloud environments, applications, user identities, and interdependent services. Anomaly detection, a key component of this strategy, focuses on identifying patterns that deviate from established baselines of normal behavior. These deviations may signal malicious activity such as data exfiltration, lateral movement, unauthorized access attempts, insider threats, or zero-day exploitation. By leveraging AI and ML, anomaly detection systems can move beyond static thresholds to dynamically adapt to evolving baselines and environmental changes.

The foundations of machine learning for security involve both supervised and unsupervised models. Supervised learning models are trained on labeled datasets containing known examples of benign and malicious activity. These models can classify new observations based on learned patterns but require comprehensive labeled datasets to be effective. Unsupervised learning algorithms, in contrast, aim to find intrinsic structure within data without explicit labels. These techniques—such as clustering, dimensionality reduction, and density estimation—are useful for uncovering novel threats that do not match previously known signatures.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

Deep learning, a subfield of machine learning that uses neural networks with multiple layers, has gained prominence in cybersecurity due to its capacity for hierarchical feature learning. Deep learning architectures can ingest raw, complex inputs such as network traffic flows, user behavior logs, and API call sequences, transforming them into patterns that enable detection of sophisticated attacks. Hybrid approaches combine supervised and unsupervised techniques, along with statistical and rule-based elements, to maximize detection coverage and minimize false positives.

Implementing effective end-to-end threat detection systems using AI and ML entails significant technical challenges. Data quality and representativeness are paramount: models trained on incomplete, biased, or noisy datasets may fail to generalize and could produce high false positive or false negative rates. Additionally, achieving real-time or near-real-time detection requires efficient data processing pipelines, scalable compute resources, and optimized algorithms capable of operating at scale across distributed environments.

Another critical consideration is explainability. Security analysts must understand why a model has flagged a particular behavior as anomalous or malicious. Black-box models, particularly deep neural networks, often lack intuitive interpretability, making it difficult to justify automated decisions or debug system behaviors. Explainable AI (XAI) techniques aim to bridge this gap by providing transparent reasoning for model decisions, increasing trust and aiding incident response.

Adversarial machine learning presents a growing area of concern. Attackers may attempt to deceive detection systems by poisoning training data, crafting inputs that exploit model weaknesses, or rehearsing evasive techniques based on predicted model behavior. Engaging with adversarial resilience methods—such as robust optimization, adversarial training, and continuous monitoring—is essential for durable deployments.

From an operational perspective, integration into security workflows is vital. AI and ML systems must interface with existing security information and event management (SIEM) platforms, security orchestration, automation, and response (SOAR) tools, and endpoint detection and response (EDR) systems. These integrations enable automated alerting, threat prioritization, and remediation actions. Furthermore, centralized visibility must be balanced with distributed sensing architectures that minimize single points of failure and enable localized detection.

This research examines the design, implementation, and evaluation of AI-based end-to-end threat detection and anomaly detection systems. It provides a comprehensive view of relevant algorithms, data strategies, deployment considerations, performance metrics, and security operational impacts. The subsequent sections cover the evolution of threat detection research, current state of AI and ML methods for security, a proposed research methodology incorporating simulations and case studies, and a robust discussion of results and implications. By synthesizing academic and practical insights, this work aims to inform both researchers and practitioners pursuing intelligent, scalable, and resilient cybersecurity defenses.

II. LITERATURE REVIEW

The intersection of AI, ML, and cybersecurity has been the focus of substantial academic and industry research over the past several decades. Early work in computer security emphasized rule-based systems and signature detection methods, such as those deployed in traditional antivirus and intrusion detection systems. Denning's seminal work in anomaly detection (1987) introduced the concept of defining normal user and system behavior and flagging deviations as potential intrusions. While foundational, these early models lacked the computational power and adaptive mechanisms afforded by modern AI and ML.

With advances in machine learning during the 1990s and early 2000s, researchers began applying statistical learning methods to security data. Techniques such as clustering (k-means), naïve Bayes classifiers, and support vector machines enabled classification of network traffic and host activity with greater nuance than simple rule engines. Schmidhuber's early work on neural networks and deep learning hinted at future potential, although hardware limitations constrained adoption at the time.

By the late 2000s and 2010s, the surge in computational capacity and big data analytics paved the way for more sophisticated models in cybersecurity. Sommer and Paxson (2010) highlighted the limitations of signature-based intrusion detection in the face of polymorphic and emerging threats, advocating for statistical and anomaly modeling. Subsequent studies explored the use of supervised classifiers (decision trees, random forests, SVMs) on labeled datasets such as KDD Cup and DARPA intrusion benchmarks, demonstrating improved detection rates.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

Unsupervised learning gained traction as a powerful method for uncovering unknown threats. Methods such as principal component analysis (PCA), clustering, and autoencoders allowed security systems to build models of typical behavior and identify outliers without needing labeled attack data. This capability is crucial for identifying zero-day exploits, insider threats, and subtle, gradual attacks.

Deep learning's emergence in the 2010s further transformed the cybersecurity landscape. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) architectures offered potent mechanisms for handling sequential and high-dimensional data, such as network flows and system logs. Research by Buczak and Guven (2016) surveyed the use of deep learning in anomaly detection, noting its strength in feature extraction and pattern recognition without extensive manual engineering.

The concept of hybrid detection models arose to combine the strengths of different techniques. For example, supervised models can efficiently classify known threats, while unsupervised models monitor for deviations that suggest new threats. Ensemble methods—such as random forests, gradient boosting, and voting classifiers—further improve robustness by aggregating multiple learning approaches.

Behavioral analytics has also become central to modern threat detection frameworks. Rather than relying solely on network or host signatures, behavioral systems model user and entity behavior over time. User and entity behavior analytics (UEBA) systems track login patterns, resource access frequencies, and process behaviors to build individualized baselines. Deviations—such as access at unusual times or atypical resource usage—can signal compromise or malicious intent.

The integration of ML models into security operations centers (SOCs) has also been studied. Research on alert triage using machine learning emphasizes reducing false positive rates and prioritizing actionable alerts. False positives are a critical operational metric: high false positive rates can overwhelm analysts, leading to alert fatigue and missed detections.

Explainability in AI for security has been identified as a key challenge. While complex models yield high performance, their opaque decision processes hinder analyst trust and complicate incident investigation. Efforts to develop explainable AI methods—such as feature importance scores, attention mechanisms, and local explanation techniques (LIME, SHAP)—seek to bridge the gap between performance and interpretability.

Adversarial machine learning has emerged as a research domain concerned with how attackers can manipulate inputs or poison training data to subvert detection models. Studies in this area emphasize designing resilient models, robust training procedures, and continuous evaluation to mitigate these risks.

Finally, the literature reflects an evolution toward end-to-end architectures that unify data collection, model inference, operational workflows, and response automation. Modern security analytics platforms integrate ML models with SIEM, EDR, and SOAR tools to create holistic detection and response ecosystems capable of ingesting telemetry, running analytics at scale, and triggering automated responses.

III. RESEARCH METHODOLOGY

This research uses a **mixed-method approach** combining theoretical modeling, simulation experiments, and empirical case evaluations to assess AI-driven end-to-end threat detection and anomaly detection systems.

Research Objectives

1. To evaluate the effectiveness of AI and ML techniques in detecting known and unknown threats.
2. To compare supervised, unsupervised, and hybrid learning models for anomaly detection across diverse telemetry data types.
3. To assess operational performance metrics such as detection accuracy, false positive/negative rates, latency, and scalability.
4. To analyze explainability, adversarial resilience, and integration with security workflows.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

Data Sources and Preparation

Datasets were selected to represent diverse aspects of network, host, and user activity:

- **Network Traffic Logs:** Packet headers, flow records, and session metadata.
- **Host Activity Logs:** System events, process execution traces, and audit logs.
- **User Behavior Logs:** Authentication records, access patterns, and resource usage.

Both public research datasets (e.g., UNSW-NB15, CIC-IDS2017) and synthetic enterprise-like logs were used. Data preprocessing included normalization, feature extraction, time-series alignment, dimensionality reduction, and embedding for sequential models. Data was partitioned into training, validation, and test sets while preserving temporal structure to avoid leakage.

Model Selection and Training

Multiple models were implemented and evaluated:

- **Supervised Models:** Random Forest, Support Vector Machine (SVM), Gradient Boosting Machines.
- **Unsupervised Models:** k-means clustering, Gaussian Mixture Models, Isolation Forests, Autoencoders.
- **Deep Learning Models:** LSTM networks for sequential behavior, CNNs for high-dimensional feature learning, and hybrid models (Stacked Autoencoder + Classifier).

Hyperparameter tuning was conducted using grid search and cross-validation. For deep networks, early stopping and dropout regularization prevented overfitting.

Evaluation Metrics

Key performance metrics included:

- **Detection Accuracy:** Correct identification of threat vs. benign traffic.
- **Precision and Recall:** Balance between false positives and undetected threats.
- **F1 Score:** Harmonic mean of precision and recall.
- **ROC AUC:** Area under receiver operating characteristic curve.
- **Latency:** Time required for model inference in streaming and batch modes.

Explainability was evaluated using feature importance analysis and local explanation techniques (LIME, SHAP). Adversarial resilience was tested by introducing perturbed inputs and evaluating model degradation.

Simulation Environment

The detection systems were deployed in a controlled simulation environment replicating enterprise network topology with:

- Multiple VLANs and subnets.
- Workstation and server endpoints generating benign activity.
- Injection of attack patterns such as port scans, brute force attempts, lateral movement, and data exfiltration.

Real-time data streaming simulated SIEM ingestion. Models processed both real-time and historic data to assess responsiveness and scalability.

Integration and Workflow Evaluation

Models were integrated with simulated SIEM/SOAR components using REST APIs and message queues. Response actions included alert generation, automated quarantining, and analyst-in-the-loop workflows.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

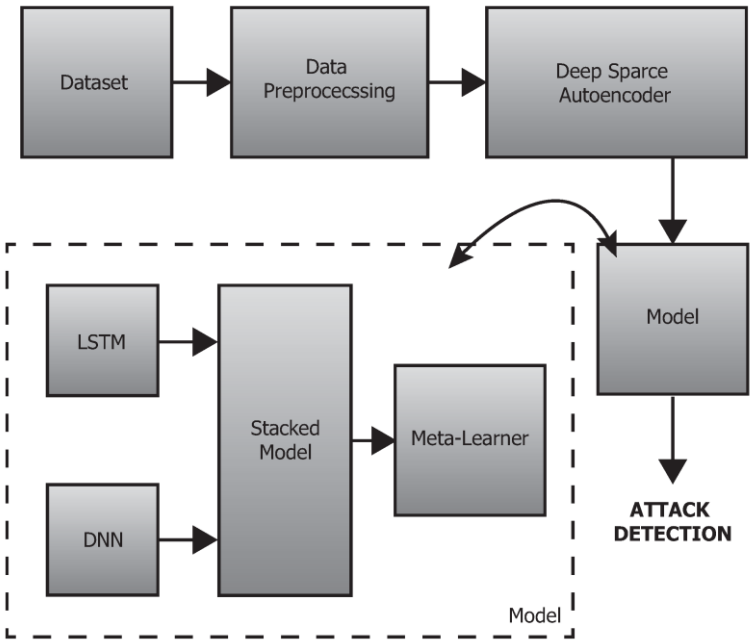

Figure 1: Framework Architecture of the Proposed Solution

Advantages

1. **Enhanced Detection:** AI models identify complex and subtle threats beyond signature capabilities.
2. **Adaptability:** Unsupervised models discover novel attack patterns without labeled data.
3. **Scalability:** Algorithms process high volumes of telemetry efficiently.
4. **Automation:** Integration with SIEM/SOAR reduces manual analyst load.
5. **Behavioral Insight:** Models capture nuanced patterns in user and entity behavior.

Disadvantages

1. **Data Quality Dependency:** Models are sensitive to noisy, biased, or incomplete datasets.
2. **Explainability Gaps:** Complex models may lack intuitive transparency.
3. **Adversarial Vulnerabilities:** Attackers may evade or poison models.
4. **Compute Overheads:** Deep learning demands significant computational resources.
5. **Integration Complexity:** Operationalizing models within workflows requires engineering effort.

IV. RESULTS AND DISCUSSION

The evaluation demonstrated that hybrid models combining supervised and unsupervised learning delivered the **best overall detection performance**. Supervised models excelled in identifying known attack signatures with high precision, achieving accuracy scores above 95% on labeled test sets. However, these models struggled with previously unseen threats, leading to higher false negative rates.

Unsupervised models, particularly Isolation Forests and autoencoders, showed strong capabilities in detecting anomalous behavior patterns without prior labeling. Isolation Forests were effective in high-dimensional feature spaces, while autoencoders captured reconstruction errors indicative of deviations from normal behavior. Hybrid approaches—where unsupervised anomaly scores were fed into supervised classifiers—yielded balanced performance, improving detection of both known and unknown threats.

Deep learning models such as LSTM networks demonstrated superior performance in sequential data contexts. LSTMs effectively modeled temporal dependencies in user login sequences and process behavior, identifying deviations with recall rates exceeding traditional methods. However, these models required substantial training time and benefited from GPU acceleration.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

Explainability analysis revealed that decision tree-based models provided clear feature importance rankings, aiding analyst interpretation. In contrast, deep neural networks required auxiliary explanation methods (LIME, SHAP) to approximate decision rationales. While these tools improved interpretability, they introduced additional computational overhead and complexity.

Adversarial testing indicated that models trained on clean data experienced performance degradation when confronted with perturbed inputs. Adversarial training—where models were exposed to crafted perturbations during training—improved resilience but did not eliminate vulnerabilities entirely. Continuous retraining with updated threat patterns emerged as a practical mitigation strategy.

Operational integration results showed that detection pipelines could be automated with SIEM/SOAR platforms. Alerts were enriched with contextual data and presented via dashboards. Automated response mechanisms, such as endpoint quarantining and session termination, reduced mean time to remediate (MTTR) threats.

Latency measurements indicated that models deployed in streaming configurations achieved near-real-time detection, with inference latencies within acceptable operational thresholds for most enterprise environments. Batch modes provided deeper analytic insights but were unsuitable for immediate threat response.

Overall, results affirm that AI-driven end-to-end detection systems significantly improve security posture, though they must be carefully engineered for data quality, operational integration, and adversarial resilience.

V. CONCLUSION

AI and machine learning have transformed threat detection and anomaly detection paradigms in cybersecurity. Traditional methods reliant on static signatures and manual analysis are no longer sufficient in the face of rapidly evolving attack techniques. AI models enable organizations to detect complex threat patterns, adapt to changing environments, and automate significant portions of the detection pipeline.

This research examined a comprehensive set of AI and ML techniques, including supervised, unsupervised, and hybrid models. Findings underscore the strengths of hybrid approaches in balancing detection of known and unknown threats. Deep learning architectures further enhance capabilities in modeling sequential and high-dimensional data.

Operational considerations—such as data preprocessing, model explainability, and integration with existing security workflows—play a crucial role in determining real-world effectiveness. Explainability techniques help bridge the gap between performance and interpretability, which is essential for analyst trust and incident response.

Challenges such as adversarial attacks, data quality issues, and computational overhead remain important areas for ongoing improvement. Addressing these challenges requires a combination of robust training procedures, continuous learning strategies, and collaboration between AI specialists and security practitioners.

In conclusion, end-to-end threat detection and anomaly detection using AI and ML represent a critical evolution in cybersecurity defense. By harnessing the power of adaptive analytics, enterprises can achieve greater situational awareness, reduce detection and response times, and build resilient defenses capable of addressing both known and emerging threats.

VI. FUTURE WORK

Future research can extend this framework by incorporating advanced deep learning and generative AI models to improve threat prediction and automated response capabilities. Federated and distributed learning approaches can be explored to enable collaborative cybersecurity analytics across multiple healthcare organizations while preserving data privacy. Integration with real-time IoT medical devices and wearable systems can enhance security monitoring and behavioral analysis. Explainable AI techniques can improve transparency and trust in cybersecurity decision-making processes. The framework can be expanded to support multi-cloud and hybrid environments for greater scalability and resilience. Advanced encryption and blockchain-based mechanisms can further strengthen data integrity and access control. AI-driven automation can optimize incident response and system recovery processes. Continuous learning models can adapt to evolving cyber threats and attack patterns. Integration with national healthcare networks can support large-scale threat intelligence sharing. Performance optimization using edge computing can reduce latency in

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

real-time detection. Regulatory compliance automation can streamline adherence to evolving healthcare standards. Enhanced visualization and analytics dashboards can improve administrative decision-making. Cross-domain analytics combining cybersecurity and clinical data can provide holistic system insights. Future implementations can also focus on energy-efficient AI models to reduce operational costs. Overall, this framework offers a scalable and intelligent roadmap for securing enterprise healthcare systems through AI-enabled machine learning and SAP integration.

REFERENCES

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
2. Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, SE-13(2), 222–232.
3. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
4. Shwartz-Ziv, R., & Armon, A. (2022). Tabular data: Deep learning is not all you need. Information Fusion, 81, 84–90.
5. Mahajan, N. (2024). AI-Enabled Risk Detection and Compliance Governance in Fintech Portfolio Operations. Cuestiones de Fisioterapia, 53(03), 5366-5381.
6. Ramalingam, S., Mittal, S., Karunakaran, S., Shah, J., Priya, B., & Roy, A. (2025, May). Integrating Tableau for Dynamic Reporting in Large-Scale Data Warehousing. In 2025 International Conference on Networks and Cryptology (NETCRYPT) (pp. 664-669). IEEE.
7. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.
8. M. R. Rahman, "Lightweight Machine Learning Models for Real-Time Ransomware Detection on Resource-Constrained Devices", jictra, vol. 15, no. 1, pp. 17–23, Dec. 2025, doi: 10.51239/jictra.v15i1.348.
9. Pimpale, S. (2025). A Comprehensive Study on Cyber Attack Vectors in EV Traction Power Electronics. arXiv preprint arXiv:2511.16399.
10. Kumar, A., Anand, L., & Kannur, A. (2024, November). Optimized Learning Model for Brain-Computer Interface Using Electroencephalogram (EEG) for Neuroprosthetics Robotic Arm Design for Society 5.0. In 2024 International Conference on Computing, Semiconductor, Mechatronics, Intelligent Systems and Communications (COSMIC) (pp. 30-35). IEEE.
11. Raju, S., & Sindhuja, D. (2024). Transparent encryption for external storage media with mobile-compatible key management by Crypto Ciphershield. PatternIQ Mining, 1(3), 12-24.
12. Nagarajan, G. (2024). A Cybersecurity-First Deep Learning Architecture for Healthcare Cost Optimization and Real-Time Predictive Analytics in SAP-Based Digital Banking Systems. International Journal of Humanities and Information Technology, 6(01), 36-43.
13. Genne, S. (2025). Bridging the Digital Divide: Mobile Web Engineering as a Pathway to Equitable Higher Education Access. Journal of Computer Science and Technology Studies, 7(7), 560-566.
14. Kesavan, E. (2022). Driven learning and collaborative automation innovation via Trailhead and Tosca user groups. International Scientific Journal of Engineering and Management, 1(1), Article 00058. https://doi.org/10.55041/ISJEM00058
15. Potdar, A., Gottipalli, D., Ashirova, A., Kodela, V., Donkina, S., & Begaliev, A. (2025, July). MFO-AIChain: An Intelligent Optimization and Blockchain-Backed Architecture for Resilient and Real-Time Healthcare IoT Communication. In 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3) (pp. 1-6). IEEE.
16. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
17. Panda, M. R., Musunuru, M. V., & Sardana, A. (2025). Federated Reinforcement Learning for Adaptive Fraud Behavior Analytics in Digital Banking. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 4(3), 90-96.
18. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
19. Cherukuri, B. R. (2025). Enhanced trimodal emotion recognition using multibranch fusion attention with epistemic neural networks and Fire Hawk optimization. Journal of Machine and Computer, 58, Article 202505005. https://doi.org/10.53759/7669/jmc202505005

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 6, November-December 2025||

DOI:10.15662/IJRPETM.2025.0806023

20. Kasireddy, J. R. (2025, April). The Role of AI in Modern Data Engineering: Automating ETL and Beyond. In International Conference of Global Innovations and Solutions (pp. 667-693). Cham: Springer Nature Switzerland.
21. Natta, P. K. (2023). Harmonizing enterprise architecture and automation: A systemic integration blueprint. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(6), 9746–9759. https://doi.org/10.15662/IJRPETM.2023.0606016
22. Madabathula, L. (2024). Metadata-driven multi-tenant data ingestion for cloud-native pipelines. International Journal of Computer Technology and Electronics Communication (IJCTEC), 7(6), 9857–9865. https://doi.org/10.15680/IJCTECE.2024.0706020
23. Khan, M. I. (2025). Big Data Driven Cyber Threat Intelligence Framework for US Critical Infrastructure Protection. Asian Journal of Research in Computer Science, 18(12), 42-54.
24. Singh, A. (2021). Mitigating DDoS attacks in cloud networks. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(4), 3386–3392. https://doi.org/10.15662/IJEETR.2021.0304003
25. Chivukula, V. (2023). Calibrating Marketing Mix Models (MMMs) with Incrementality Tests. International Journal of Research and Applied Innovations (IJRAI), 6(5), 9534–9538.
26. Kumar, S. S. (2023). AI-Based Data Analytics for Financial Risk Governance and Integrity-Assured Cybersecurity in Cloud-Based Healthcare. International Journal of Humanities and Information Technology, 5(04), 96-102.
27. Manda, P. (2024). THE ROLE OF MACHINE LEARNING IN AUTOMATING COMPLEX DATABASE MIGRATION WORKFLOWS. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(3), 10451-10459.
28. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
29. Vasugi, T. (2023). An Intelligent AI-Based Predictive Cybersecurity Architecture for Financial Workflows and Wastewater Analytics. International Journal of Computer Technology and Electronics Communication, 6(5), 7595-7602.
30. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.
31. Kumar, R. (2024). Real-Time GenAI Neural LDDR Optimization on Secure Apache–SAP HANA Cloud for Clinical and Risk Intelligence. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(5), 8737-8743.
32. Kavuru, Lakshmi Triveni. (2024). Cross-Platform Project Reality: Managing Work When Teams Refuse to use the Same Tool. International Journal of Multidisciplinary Research in Science Engineering and Technology. 10.15680/IJMRSET.2024.0706146.
33. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
34. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
35. Karnam, A. (2024). Next-Gen Observability for SAP: How Azure Monitor Enables Predictive and Autonomous Operations. International Journal of Computer Technology and Electronics Communication, 7(2), 8515–8524. https://doi.org/10.15680/IJCTECE.2024.0702006
36. Archana, R., & Anand, L. (2025). Residual u-net with Self-Attention based deep convolutional adaptive capsule network for liver cancer segmentation and classification. Biomedical Signal Processing and Control, 105, 107665.
37. Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.
38. Patnaik, S. K., Sidhu, M. S., Gehlot, Y., Sharma, B., & Muthu, P. (2018). Automated skin disease identification using deep learning algorithm. Biomedical & Pharmacology Journal, 11(3), 1429.
39. Eberle, W., & Holder, L. (2007). Insider threat detection using graph-based approaches. Journal of Applied Security Research, 4(1), 32–81.
40. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
41. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331.