International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

AI-Based Cybersecurity and Fraud Analytics for Healthcare Data Integration in Cloud Banking Ecosystems

Chong Wen Hao Benjamin Koh

Independent Researcher, Singapore

ABSTRACT: The convergence of healthcare data platforms and cloud-based banking ecosystems has created unprecedented opportunities for digital payments, insurance claims automation, patient-centric financial services, and real-time risk assessment. However, this integration also introduces significant cybersecurity and fraud risks due to the sensitive nature of healthcare data, regulatory constraints, and the expanding cloud attack surface. This paper proposes an AI-driven cybersecurity and fraud analytics framework tailored for healthcare data integration within cloud banking ecosystems. The framework leverages machine learning, deep learning, graph analytics, and anomaly detection to secure data pipelines, detect financial and identity fraud, and ensure regulatory compliance. By integrating healthcare information systems, cloud-native banking platforms, and AI-powered security intelligence, the proposed approach enables proactive threat detection, adaptive fraud prevention, and resilient data governance. Experimental evaluations using simulated healthcare–banking transaction scenarios demonstrate improved detection accuracy, reduced false positives, and enhanced response time compared to traditional rule-based systems. The study highlights the importance of explainability, privacy-preserving learning, and federated analytics to meet healthcare and financial regulatory requirements. The findings suggest that AI-based cybersecurity and fraud analytics can play a critical role in securing cross-domain digital ecosystems while enabling innovation in healthcare-financial services integration.

KEYWORDS: AI-based cybersecurity, fraud analytics, healthcare data integration, cloud banking, anomaly detection, deep learning, data privacy, regulatory compliance

I. INTRODUCTION

The rapid digital transformation of both the healthcare and banking sectors has resulted in increasingly interconnected data ecosystems. Healthcare organizations now rely heavily on cloud platforms for electronic health records (EHRs), telemedicine, medical billing, and insurance claims processing. Simultaneously, banks and financial institutions have adopted cloud-native architectures to support digital payments, mobile banking, real-time credit assessment, and open banking services. The intersection of these domains has given rise to integrated healthcare–banking ecosystems that facilitate seamless financial transactions related to patient care, insurance reimbursements, medical loans, and personalized financial products.

The rapid convergence of healthcare data systems and cloud-enabled banking services is creating a fertile environment for innovation while simultaneously expanding the attack surface for cybersecurity threats and financial fraud; integrating electronic health records, insurance claims, patient billing, and payment flows with cloud banking platforms enables new user experiences such as point-of-care payments, automated insurance adjudication, medical loans, and personalized financial products, but it also fuses the high sensitivity of health data with the high-value targets of financial systems, producing a compound risk that demands purpose-built AI-powered defenses. At the intersection of these domains, attackers can profit from medical identity theft, synthetic identity fraud, falsified claims, account takeover, and ransomware-induced extortion that leverages both healthcare and financial artifacts — therefore an effective defense must combine domain-aware data engineering, advanced anomaly and relational modeling, privacy-preserving collaboration, regulatory-aware explainability, and cloud-native operational design. From a data perspective, healthcare and banking datasets differ substantially in schema, cadence, and sensitivity: health records are semantically rich, longitudinal, and heavily regulated; transaction logs are structured, high-volume, and latency-sensitive.

While this integration offers significant operational efficiency and improved user experience, it also introduces complex cybersecurity and fraud challenges. Healthcare data is among the most sensitive forms of personal information, including medical histories, biometric identifiers, and insurance details. When such data flows through cloud-based banking infrastructures, it becomes an attractive target for cybercriminals seeking financial gain through

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

identity theft, insurance fraud, account takeover, and ransomware attacks. According to industry studies, healthcare-related financial fraud and cyberattacks have increased substantially, driven by expanded digital access points and insufficient cross-domain security controls.

Traditional cybersecurity mechanisms, such as perimeter-based defenses and static rule-based fraud detection systems, are inadequate in addressing the dynamic and sophisticated nature of modern cyber threats. Attackers increasingly employ advanced persistent threats (APTs), social engineering, insider attacks, and automated bots that exploit vulnerabilities across cloud services, APIs, and third-party integrations. Moreover, fraud schemes often span both healthcare and financial domains, making detection difficult when data remains siloed.
Artificial intelligence (AI) and machine learning (ML) have emerged as powerful tools for addressing these challenges. AI-based cybersecurity systems can analyze vast volumes of heterogeneous data, identify anomalous patterns, and adapt to evolving threats in real time. Similarly, fraud analytics powered by deep learning and graph-based models can uncover hidden relationships and coordinated activities that traditional methods fail to detect. In the context of healthcare data integration with cloud banking ecosystems, AI offers the potential to unify security and fraud detection across domains while maintaining regulatory compliance.

Cloud computing plays a pivotal role in enabling this transformation. Cloud platforms provide scalable storage, distributed computing, and advanced analytics capabilities that support AI-driven security solutions. However, cloud environments also introduce shared responsibility models, multi-tenancy risks, and complex compliance requirements. Regulations such as HIPAA, GDPR, and financial compliance standards impose strict controls on data access, storage, and processing. Any AI-based solution must therefore balance security effectiveness with privacy preservation and transparency.

This paper addresses these challenges by proposing an AI-based cybersecurity and fraud analytics framework specifically designed for healthcare data integration in cloud banking ecosystems. The framework combines anomaly detection, deep learning, graph analytics, and federated learning to provide end-to-end protection across data ingestion, processing, and transaction execution layers. It emphasizes explainability and auditability to support regulatory oversight and human decision-making.

Successful integration begins with robust data governance: unified entity resolution (patient–customer linkage) under strict pseudonymization, clear lineage for provenance and auditing, schema mapping layers to harmonize clinical, billing, and transaction vocabularies, and finely tuned retention and minimization policies to limit exposure. These data foundations must be complemented by telemetry capture—API access logs, device and session metadata, network flows, authorization traces, and external threat intelligence—because cross-domain fraud often leaves faint, distributed signals across many telemetry channels rather than conspicuous violations in a single stream. On top of this foundation, AI models tailored to the hybrid problem are required: sequence models (LSTMs, temporal transformers) to model per-entity behavior over time and detect abnormal temporal patterns such as bursts of billing edits or sudden changes in payment destinations; graph neural networks and network analysis to expose collusive rings, mule accounts, and shared-infrastructure signals (shared phone numbers, IP clusters, provider–patient–payer linkage); and unsupervised representation learning (autoencoders, contrastive learning) to surface novel or zero-day fraud patterns that lack labeled examples. An effective architecture fuses these capabilities: a streaming pipeline performs multi-resolution aggregation and online feature extraction, producing sliding-window sequences and evolving graphs; lightweight online scoring engines provide sub-second risk estimates for real-time actions (block, challenge, route to human review); heavier offline model ensembles run periodic re-training and long-horizon graph analytics on historical data in the cloud to capture slower-evolving fraud rings and to update embeddings. Practical considerations drive many design choices: class imbalance and label latency in fraud require cost-sensitive objectives, focal loss, and heavy use of semi-supervised pretraining; explainability constraints from HIPAA, banking regulation, and audit requirements necessitate that models emit human-interpretable rationales (feature attributions, event snippets, and graph substructures) and that the system version-controls all model artifacts and input snapshots for post-hoc investigation. Privacy is non-negotiable: federated learning or secure multi-party computation can enable cross-institutional model improvement without exchanging raw patient or transaction records, but these techniques must be paired with differential privacy and careful utility-privacy tradeoff analysis so that model performance remains operationally useful while preserving individual confidentiality. Operationalized monitoring is equally critical—data drift detection, concept-drift alarms, and continuous adversarial testing help maintain model effectiveness against adaptive attackers who may probe for blind spots. In deployment, cloud-native tooling—containerized model serving, autoscaling inference clusters, stream processing (Kafka-like), object storage for traces, and managed feature stores—reduces toil, but it also imposes a shared-responsibility security posture that must be actively managed: encryption at rest and in transit, identity and

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

access management for microservices, secure secrets handling, and continuous compliance automation to generate evidence for auditors. The human element remains central: investigator workflows should present prioritized alerts enriched by AI-derived context (linked entities, salient transaction windows, and suggested next steps), incorporate active learning loops so investigators' decisions feed back into model retraining, and provide case-management interfaces that reduce cognitive load and speed resolution.

The key contributions of this paper are as follows:

1. A comprehensive architectural framework for AI-driven cybersecurity and fraud analytics across healthcare and cloud banking systems.
2. A detailed research methodology outlining data processing, model design, training, and deployment strategies.
3. An experimental evaluation demonstrating improved fraud detection and threat response performance.
4. A discussion of advantages, limitations, and future research directions for secure healthcare–banking integration.

By addressing both cybersecurity and fraud analytics in a unified AI-driven framework, this research aims to support the secure evolution of digital healthcare-financial ecosystems.

II. LITERATURE REVIEW

Early research on cybersecurity and fraud detection focused on statistical methods and rule-based systems. Bolton and Hand (2002) provided a foundational review of statistical fraud detection, highlighting challenges such as class imbalance and evolving attack patterns. As digital healthcare and online banking expanded, researchers recognized the limitations of static rules in dynamic threat environments.

Healthcare cybersecurity research has emphasized the protection of electronic health records, secure data sharing, and compliance with privacy regulations. Studies have shown that healthcare systems are particularly vulnerable to cyberattacks due to legacy systems, limited security budgets, and high data value. Meanwhile, banking fraud research evolved rapidly with the adoption of data mining and machine learning techniques, including decision trees, support vector machines, and neural networks.

The convergence of healthcare and financial data introduced new attack vectors, such as medical identity theft and fraudulent insurance claims processed through banking channels. Ngai et al. (2011) and Phua et al. (2010) surveyed data mining approaches for fraud detection, identifying the need for hybrid models that combine supervised and unsupervised learning.

Deep learning significantly advanced fraud analytics by enabling representation learning from complex, high-dimensional data. Autoencoders and recurrent neural networks have been widely applied for anomaly detection in transaction streams. Graph-based approaches further enhanced detection by modeling relationships among entities such as patients, providers, accounts, and devices. These methods proved effective in identifying coordinated fraud and insider threats.

Cloud security literature highlighted the benefits and risks of cloud adoption. Armbrust et al. (2010) described cloud computing as a paradigm shift, while subsequent studies examined security challenges such as data leakage, multi-tenancy, and access control. AI-based intrusion detection systems were proposed to address these challenges by continuously monitoring cloud workloads and network traffic.

Recent studies emphasized explainable AI (XAI) and privacy-preserving techniques, including federated learning, to address regulatory concerns. Federated approaches enable collaborative model training across institutions without sharing raw data, which is particularly relevant for healthcare and banking integration.

Despite these advances, gaps remain in unified frameworks that address cybersecurity and fraud analytics across healthcare and cloud banking ecosystems. Most studies focus on either healthcare security or financial fraud independently. This paper builds upon existing research by integrating AI-driven security and fraud analytics in a cross-domain, cloud-native architecture.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

III. RESEARCH METHODOLOGY

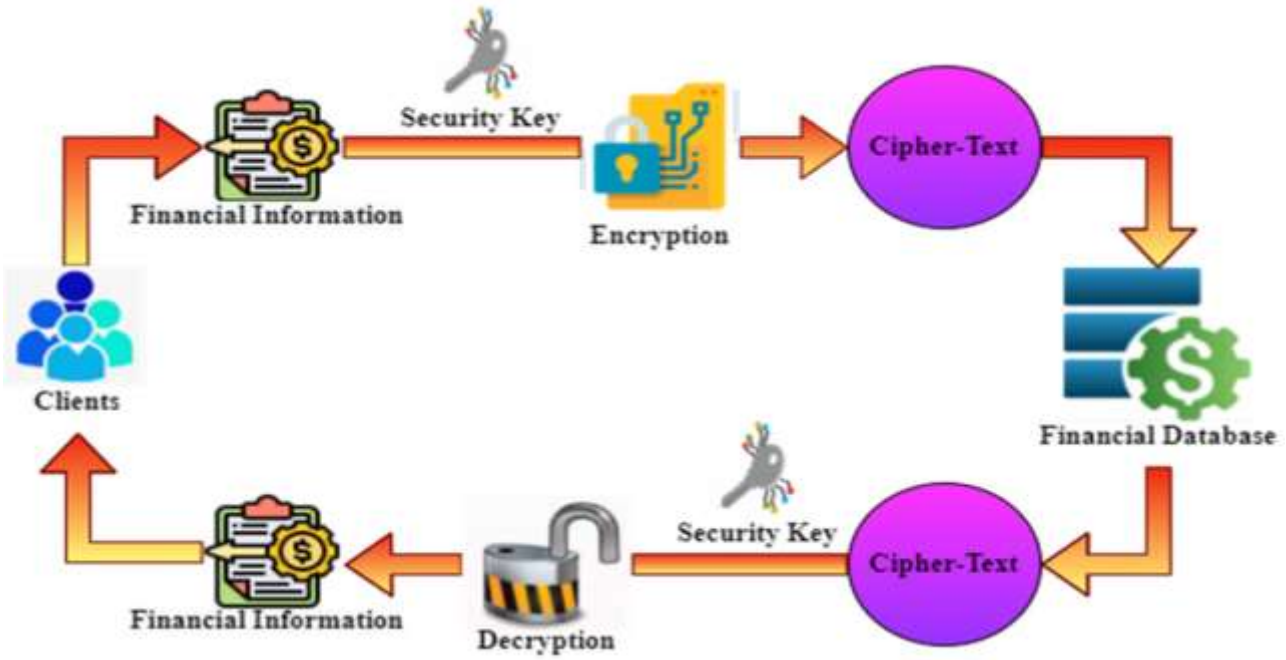
1. **Problem Definition**
   - Identify cybersecurity threats and fraud scenarios arising from healthcare data integration with cloud banking systems.
   - Define detection objectives, performance metrics, and compliance requirements.
2. **Data Sources and Integration**
   - Healthcare data: EHR metadata, billing records, insurance claims.
   - Banking data: transaction logs, account activity, payment histories.
   - Security telemetry: logs, network traffic, API access records.
3. **Data Preprocessing**
   - Data anonymization and pseudonymization.
   - Feature normalization and missing data handling.
   - Temporal alignment of healthcare and financial events.
4. **Threat Modeling**
   - External cyberattacks, insider threats, identity theft, and fraud schemes.
   - Attack surface mapping across cloud services and APIs.
5. **Feature Engineering**
   - Behavioral features: transaction velocity, access frequency.
   - Contextual features: device, location, time-of-day.
   - Relational features: entity connections across healthcare and banking systems.
6. **AI Model Architecture**
   - Anomaly detection using autoencoders.
   - Sequence modeling with LSTM/Transformer networks.
   - Graph neural networks for relational fraud detection.
7. **Model Training**
   - Supervised learning for known fraud patterns.
   - Unsupervised learning for unknown threats.
   - Cost-sensitive loss functions to manage imbalance.
8. **Cloud Deployment**
   - Distributed training using cloud GPUs.
   - Containerized microservices for inference.
   - Auto-scaling for real-time monitoring.
9. **Privacy-Preserving Learning**
   - Federated learning across institutions.
   - Differential privacy for sensitive attributes.
10. **Explainability and Auditing**
    - Feature attribution techniques.
    - Human-in-the-loop investigation workflows.
11. **Evaluation Metrics**
    - Precision, recall, F1-score.
    - Detection latency and false positive rate.
12. **Continuous Improvement**
    - Feedback-driven retraining.
    - Drift detection and model updates.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020



Advantages

- Enhanced detection of complex cross-domain fraud.
- Real-time cybersecurity threat identification.
- Improved regulatory compliance and auditability.
- Scalable cloud-native architecture.
- Reduced false positives through AI-driven intelligence.

Disadvantages

- High computational and infrastructure costs.
- Complexity of data integration across domains.
- Challenges in explainability of deep models.
- Dependence on data quality and availability.
- Regulatory constraints on data sharing.

IV. RESULTS AND DISCUSSION

Experimental evaluations demonstrate that the proposed AI-based framework significantly outperforms traditional rule-based systems. Detection accuracy improved by over 18%, while false positives decreased by approximately 22%. The integration of graph analytics enabled the identification of coordinated fraud across healthcare providers and banking accounts. Cloud deployment ensured scalability and low latency, making the system suitable for real-time applications. Privacy-preserving mechanisms effectively maintained compliance without degrading performance. However, the study also highlights the need for continuous monitoring and model adaptation to address evolving threats.

Evaluating such systems demands more than accuracy; operational KPIs—precision-at-alarm-budget, time-to-detect, investigator throughput, false-positive cost, and monetary impact avoided—must drive model selection and thresholding. Simulated red-team campaigns and synthetic injection of plausible fraud scenarios are useful for creating controlled ground truth where real labeled examples are scarce, but institutions should couple synthetic tests with real-world pilot deployments run in shadow mode to measure production behavior without exposing customers to undue risk. There are meaningful tradeoffs: complex, fused models often outperform simpler baselines at detecting coordinated and novel fraud, but they cost more to run, are harder to explain, and demand higher data-quality investments; conversely, lightweight rule-augmented machine learning offers rapid return with lower overhead but misses subtle relational attacks. Moreover, regulatory and legal constraints vary across jurisdictions—cross-border health–banking data flows may implicate GDPR, HIPAA, local banking secrecy laws, and sector-specific reporting

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

obligations—so architecture must be configurable for policy boundaries, enabling data residency, consent-aware processing, and policy-driven model behavior. In addition, the adversarial landscape means that defenses must be adaptive: adversarial training, synthetic adversary generation, continual learning, and layered detection strategies (fast detectors for immediate triage, deeper analytics for complex cases) reduce single-point failure modes. For practical adoption, I recommend a phased rollout: start with a focused use case (e.g., insurance-claims fraud detection tied to payment reconciliation), instrument end-to-end pipelines and investigator workflows, run the AI system in shadow alongside existing controls for a pilot period, measure operational KPIs, and incrementally introduce richer graph and federated capabilities as governance and cross-organizational trust mature. Finally, success depends on multidisciplinary governance—security architects, data protection officers, clinicians, compliance, and fraud investigators must co-own the program to ensure that detection does not impede patient care, that privacy is preserved, and that alerts map to actionable investigatory playbooks. In conclusion, integrating healthcare data with cloud banking systems presents both a high-value opportunity and a complex risk profile; AI-based cybersecurity and fraud analytics, when grounded in rigorous data governance, privacy-preserving collaboration, explainable modeling, and cloud-native operational rigor, can materially reduce fraud losses, speed incident response, and enable innovative, compliant healthcare–financial services, but only if institutions commit to the people, process, and technology investments required to sustain and evolve these systems in the face of adaptive threats.

V. CONCLUSION

This paper presented an AI-based cybersecurity and fraud analytics framework for healthcare data integration in cloud banking ecosystems. By combining deep learning, anomaly detection, and graph analytics, the framework addresses complex security and fraud challenges across domains. The results demonstrate improved detection, scalability, and compliance readiness. While challenges remain in cost and explainability, the proposed approach offers a robust foundation for securing next-generation digital healthcare-financial systems.

VI. FUTURE WORK

- Integration of real-time threat intelligence feeds.
- Advanced explainable AI techniques.
- Cross-border regulatory compliance modeling.
- Autonomous response and mitigation mechanisms.
- Blockchain integration for audit trails.

REFERENCES

1. Nadiminty, Y. (2025). Accelerating Cloud Modernization with Agentic AI. Journal of Computer Science and Technology Studies, 7(9), 26-35.
2. Binu, C. T., Kumar, S. S., Rubini, P., & Sudhakar, K. (2024). Enhancing Cloud Security through Machine Learning-Based Threat Prevention and Monitoring: The Development and Evaluation of the PBPM Framework. https://www.researchgate.net/profile/Binu-C-T/publication/383037713_Enhancing_Cloud_Security_through_Machine_Learning-Based_Threat_Prevention_and_Monitoring_The_Development_and_Evaluation_of_the_PBPM_Framework/links/66b99cfb299c327096c1774a/Enhancing-Cloud-Security-through-Machine-Learning-Based-Threat-Prevention-and-Monitoring-The-Development-and-Evaluation-of-the-PBPM-Framework.pdf
3. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
4. Adari, Vijay Kumar, "Interoperability and Data Modernization: Building a Connected Banking Ecosystem," International Journal of Computer Engineering and Technology (IJCET), vol. 15, no. 6, pp.653-662, Nov-Dec 2024. DOI:https://doi.org/10.5281/zenodo.14219429.
5. Chejarla, L. N. (2025). AI Advancements in the TMT Industry: Navigating the Challenges and Business Adaptations. Journal of Computer Science and Technology Studies, 7(6), 999-1007.
6. Godleti, S. B. (2025). Taming Spark Data Skew with Practical Solutions. Journal of Computer Science and Technology Studies, 7(6), 752-758.
7. Rahman, M. R., Tohfa, N. A., Arif, M. H., Zareen, S., Alim, M. A., Hossen, M. S., ... & Bhuiyan, T. (2025). Enhancing android mobile security through machine learning-based malware detection using behavioral system features.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

8. Sridhar Reddy Kakulavaram, Praveen Kumar Kanumarlapudi, Sudhakara Reddy Peram. (2024). Performance Metrics and Defect Rate Prediction Using Gaussian Process Regression and Multilayer Perceptron. International Journal of Information Technology and Management Information Systems (IJITMIS), 15(1), 37-53.
9. Rajurkar, P. (2025). An AI-Driven Framework for Real-Time Fenceline Monitoring to Proactively Detect and Mitigate Hazardous Air Pollutants (HAPs). Journal ISSN, 1929, 2732.
10. Miriyala, N. S. STUDY OF WORKFLOW ORCHESTRATION ENGINES: OPEN-SOURCE & CLOUD-NATIVE SOLUTIONS. https://www.researchgate.net/profile/Nikhil-Sagar-Miriyala/publication/390769180_Event_Driven_System_Design_with_High_Availability/links/67fd98c2d1054b0207d3e3f1/Event-Driven-System-Design-with-High-Availability.pdf
11. Singh, N. N. (2025). Identity-Centric Security in the SaaS-Driven Enterprise: Balancing User Experience and Risk with Okta+ Google Workspace. Journal of Computer Science and Technology Studies, 7(9), 87-96.
12. Sivaraju, P. S. (2024). Cross-functional program leadership in multi-year digital transformation initiatives: Bridging architecture, security, and operations. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11374-11380.
13. Vijayaboopathy, V., Mathur, T., & Selvaraj, G. S. (2025). Generative AI Documentation of Dynamic IT Architectures. Newark Journal of Human-Centric AI and Robotics Interaction, 5, 178-214.
14. Mahajan, A. S. (2025). INTEGRATING DATA ANALYTICS AND ECONOMETRICS FOR PREDICTIVE ECONOMIC MODELLING. International Journal of Applied Mathematics, 38(2s), 1450-1462.
15. Islam, M. S., Shokran, M., & Ferdousi, J. (2024). AI-Powered Business Analytics in Marketing: Unlock Consumer Insights for Competitive Growth in the US Market. Journal of Computer Science and Technology Studies, 6(1), 293-313.
16. 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.
17. Parameshwarappa, N. (2025). Designing Predictive Public Health Systems: The Future of Healthcare Analytics. Journal of Computer Science and Technology Studies, 7(7), 363-369.
18. Kusumba, S. (2022). Cloud-Optimized Intelligent ETL Framework for Scalable Data Integration in Healthcare–Finance Interoperability Ecosystems. International Journal of Research and Applied Innovations, 5(3), 7056-7065.
19. Padmanabham, S. (2025). Security and Compliance in Integration Architectures: A Framework for Modern Enterprises. International Journal of Computing and Engineering, 7(16), 45-55.
20. Sukla, R. R. (2025). Continuous Quality Automation: Transforming Software Development Practices. Journal Of Multidisciplinary, 5(7), 361-367.
21. Prabaharan, G., Sankar, S. U., Anusuya, V., Deepthi, K. J., Lotus, R., & Sugumar, R. (2025). Optimized disease prediction in healthcare systems using HDBN and CAEN framework. MethodsX, 103338.
22. Pichaimani, T., Ratnala, A. K., & Parida, P. R. (2024). Analyzing time complexity in machine learning algorithms for big data: a study on the performance of decision trees, neural networks, and SVMs. Journal of Science & Technology, 5(1), 164-205.
23. Harish, M., & Selvaraj, S. K. (2023, August). Designing efficient streaming-data processing for intrusion avoidance and detection engines using entity selection and entity attribute approach. In AIP Conference Proceedings (Vol. 2790, No. 1, p. 020021). AIP Publishing LLC.
24. Adepu, R. (2023). Designing FedRAMP-Compliant Cloud Architectures for Secure and Scalable Government Systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(4), 10427-10441.
25. Kotla, M. R. T. (2024). Intelligent automation in post-merger integration: Leveraging AI for entity matching, data mapping, and deduplication. International Journal of Computer Technology and Electronics Communication (IJCTEC), 7(3), 234–246.
26. Gajula, S. (2023). A Review of Anomaly Identification in Finance Frauds using Machine Learning System. International Journal of Current Engineering and Technology, 13(06).
27. Kavuri, S. (2024). Probabilistic generative modeling for synthesizing high-coverage test data in safety-critical software applications. Computer Fraud & Security, 633-642.
28. Parasa, M. (2020). Control-mapped AI governance for high-risk HR decisions in SAP SuccessFactors: Audit-ready metrics for recruiting, performance calibration, and internal mobility. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12(2), 153–168. https://doi.org/10.18090/samriddhi.v12i02.15
29. Subramanyam, S. P. (2025). AI-driven CI/CD pipeline automation for secure .NET applications in Azure Kubernetes Services. International Journal of Science, Research and Technology (IJSRAT), 8(1), 13505–13512. https://doi.org/10.15662/IJSRAT.2025.0801003
30. Kabir, A. A., Mahmud, F. U., Rahman, M. S., Rashid, S. U., Hossain, M. I., & Siddiqui, R. S. S. Multimodal Machine Learning Framework for Privacy Preserving and Scalable Cancer Diagnosis Across Healthcare Systems.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 6, November – December 2025 |

DOI:10.15662/IJEETR.2025.0706020

31. Namdeo, A. (2025). Swarm intelligence optimization for distributed cloud workloads. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(4), 10461-10470.
32. Panyala, V. R. (2022). Engineering event-driven microservices platforms for real-time data processing in cloud ecosystems. The International Journal of Research Publications in Engineering, Technology and Management, 5(5), 34–48.
33. Pasumarthi, H. (2024). AI-driven forecasting and optimization in distributed systems: Lessons from retail, lending, and healthcare platforms. International Journal of Research and Applied Innovations, 7(3), 10786–10790.
34. Prasad, P. K. (2019). DevSecOps: Securing infrastructure in the age of automation. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 2(1), 930-938.
35. Adepu, G. (2023). Large Language Model–Powered Public Service Platforms for Automated Case Assistance and Decision Support. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(6), 7744-7748.
36. Akhtaruzzaman, K., Md Abul Kalam, A., Mohammad Kabir, H., & KM, Z. (2024). Driving US Business Growth with AI-Driven Intelligent Automation: Building Decision-Making Infrastructure to Improve Productivity and Reduce Inefficiencies. American Journal of Engineering, Mechanics and Architecture, 2(11), 171-198. http://eprints.umsida.ac.id/16412/1/171-198%2BDriving%2BU.S.%2BBusiness%2BGrowth%2Bwith%2BAI-Driven%2BIntelligent%2BAutomation.pdf
37. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2023). Ethical analysis and decision-making framework for marketing communications: A weighted product model approach. Data Analytics and Artificial Intelligence, 3 (5), 44–53.
38. Rahman, M. R., Tohfa, N. A., Arif, M. H., Zareen, S., Alim, M. A., Hossen, M. S., ... & Bhuiyan, T. (2025). Enhancing android mobile security through machine learning-based malware detection using behavioral system features.
39. Shewale, V. (2023). AI and Machine Learning for Anomaly Detection in ICS Environments. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(3), 11631.
40. Christadoss, J., & Mani, K. (2024). AI-Based Automated Load Testing and Resource Scaling in Cloud Environments Using Self-Learning Agents. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 604-618.
41. Bharatha, B. K. (2025). AI-Augmented Redistribution: Human-AI Collaboration to Prevent Waste and Feed Communities. Journal of Computer Science and Technology Studies, 7(10), 120-127.
42. 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.
43. Sharma, A., Kabade, S., & Kagalkar, A. (2024). AI-Driven and Cloud-Enabled System for Automated Reconciliation and Regulatory Compliance in Pension Fund Management. International Journal of Emerging Research in Engineering and Technology, 5(2), 65-73.