International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804014

Next Generation Intelligent Cloud Framework for Secure Digital Banking Healthcare and Government Infrastructure

Hari Sangeetham

Senior Solution Specialist, Deloitte, United States

ABSTRACT: The rapid digital transformation in banking, healthcare, and government sectors has accelerated the adoption of cloud computing to support scalable, flexible, and resilient services. However, these infrastructures are increasingly exposed to cyber threats, regulatory compliance challenges, and complex operational demands. This research proposes a next-generation intelligent cloud framework designed to provide secure, efficient, and reliable services for digital banking, healthcare, and government infrastructures. The framework integrates artificial intelligence (AI), machine learning (ML), and advanced security mechanisms to enable predictive threat detection, dynamic resource management, and adaptive risk mitigation. Core components include AI-driven anomaly detection, multi-layer encryption, identity and access management, and real-time monitoring. The proposed framework is evaluated using simulated digital banking, healthcare, and government datasets, demonstrating improvements in security, service availability, and operational efficiency compared to traditional cloud architectures. Experimental results indicate a reduction in potential security breaches, enhanced compliance with regulatory standards such as GDPR, HIPAA, and PCI DSS, and optimized resource utilization. This research provides a comprehensive blueprint for deploying intelligent, secure, and resilient cloud systems capable of supporting mission-critical digital services in highly regulated environments.

KEYWORDS: Intelligent Cloud Framework, Secure Cloud Computing, Digital Banking, Healthcare IT, Government Infrastructure, AI-Driven Security, Predictive Threat Detection, Cloud Resource Optimization, Regulatory Compliance, Cybersecurity

I. INTRODUCTION

Cloud computing has revolutionized the delivery of digital services across banking, healthcare, and government sectors by providing scalable, flexible, and cost-efficient infrastructure. Digital banking platforms rely on cloud environments to manage transactions, customer data, and real-time financial analytics. Healthcare organizations leverage cloud computing to store electronic health records (EHRs), coordinate care, and support telemedicine services. Government agencies utilize cloud infrastructure to deliver citizen services, manage sensitive records, and implement large-scale data analytics for policy and operational decisions. Despite the operational advantages, cloud adoption in these sectors faces significant challenges related to security, compliance, high availability, and resource optimization.

Digital banking, for instance, handles sensitive financial data that is constantly targeted by cyberattacks such as phishing, ransomware, and fraud schemes. Cloud-native banking systems require advanced threat detection, identity management, and data protection mechanisms to ensure both operational integrity and customer trust. Healthcare systems face strict regulatory requirements, including HIPAA, GDPR, and local privacy laws, making secure data handling a critical concern. Moreover, healthcare infrastructure must support high availability and reliability to ensure uninterrupted patient care. Government systems similarly demand robust security protocols, continuous monitoring, and regulatory compliance to maintain citizen trust and protect critical national information.

Traditional cloud frameworks often rely on static security measures and manual monitoring, which are insufficient to meet the demands of modern digital infrastructures. Cyber threats are increasingly sophisticated, dynamic, and capable of bypassing conventional defenses. Furthermore, the scale of data generated in banking, healthcare, and government operations requires intelligent mechanisms for predictive monitoring, anomaly detection, and automated resource management. Without such mechanisms, organizations risk service disruptions, data breaches, and regulatory violations, all of which can have significant operational, financial, and reputational consequences.

This research introduces a next-generation intelligent cloud framework that integrates artificial intelligence (AI), machine learning (ML), and advanced security protocols to address these challenges. The framework emphasizes predictive threat detection, automated anomaly response, dynamic resource allocation, and compliance adherence. AI models are employed to analyze real-time system logs, transaction data, and operational metrics to identify anomalies, forecast potential threats, and trigger automated mitigation actions. Machine learning algorithms optimize resource utilization, ensuring high availability and operational efficiency across cloud-hosted applications.

The proposed framework also incorporates a multi-layered security approach. Data encryption, secure communication protocols, and identity and access management are employed to protect sensitive banking, healthcare, and government data. Regulatory compliance is enforced through policy-driven controls, audit logging, and automated reporting, enabling organizations to meet legal and operational standards without compromising service performance. Additionally, predictive analytics supports proactive maintenance and dynamic scaling, reducing downtime and optimizing operational costs.

By integrating intelligent automation with robust security measures, the framework provides a unified architecture capable of supporting mission-critical operations in highly regulated environments. The research evaluates the framework using simulated datasets representing banking transactions, healthcare records, and government operations, assessing security, availability, performance, and compliance outcomes. The results demonstrate the framework's ability to enhance threat detection, reduce operational risks, and improve resource efficiency compared to conventional cloud implementations.

In conclusion, the adoption of intelligent cloud frameworks represents a strategic imperative for digital banking, healthcare, and government organizations. By combining AI-driven analytics, predictive threat detection, and secure cloud operations, the proposed framework offers a resilient, compliant, and efficient solution for managing complex digital infrastructures. The remainder of this research provides an in-depth review of related work, methodology for framework development and validation, and an analysis of advantages and limitations of the approach.

II. LITERATURE REVIEW

Research on intelligent cloud frameworks emphasizes the integration of AI, ML, and advanced security mechanisms to enhance cloud service reliability and security. Studies by Zhang et al. (2019) demonstrate the use of predictive analytics for anomaly detection in financial cloud systems, significantly reducing fraudulent transactions and cyberattack incidents. Similarly, research in healthcare IT by Li et al. (2020) highlights AI-driven monitoring of EHR systems to identify suspicious access patterns, ensuring compliance with HIPAA regulations while maintaining patient care continuity.

Government cloud infrastructure has been the focus of numerous studies exploring the challenges of large-scale, sensitive data management. Research by Kumar et al. (2018) identifies predictive threat detection and automated resource allocation as key enablers of secure and resilient digital governance platforms. Studies also emphasize multi-layered security architectures combining encryption, access controls, and AI-based monitoring to prevent unauthorized access and data breaches.

While conventional cloud platforms provide scalability and cost efficiency, they often lack proactive threat detection and automated operational intelligence. AI-based cloud frameworks address these gaps by employing supervised and unsupervised learning models for anomaly detection, resource optimization, and compliance enforcement. Techniques such as ensemble learning, reinforcement learning, and explainable AI enhance predictive accuracy and operational transparency.

Despite these advances, challenges remain in integrating intelligent frameworks into highly regulated sectors. Banking, healthcare, and government infrastructures generate heterogeneous, high-volume data requiring robust preprocessing, normalization, and feature engineering. Real-time monitoring and automated decision-making demand low-latency computation, while regulatory requirements necessitate transparency, auditability, and secure data handling. Recent research emphasizes hybrid frameworks combining AI analytics, secure cloud orchestration, and multi-tenant isolation to meet these operational and compliance needs.

In summary, existing literature supports the need for next-generation intelligent cloud frameworks that integrate predictive AI, automated operations, and robust security to meet the demands of digital banking, healthcare, and government infrastructures. However, gaps remain in holistic frameworks capable of addressing security, compliance, scalability, and operational efficiency simultaneously.

III. RESEARCH METHODOLOGY

Research Design

Experimental and analytical approach to develop an intelligent cloud framework integrating AI, ML, and advanced security for banking, healthcare, and government systems.

Data Collection

Simulation datasets include financial transactions, healthcare records, and government operational data. Historical logs and telemetry data collected for predictive modeling.

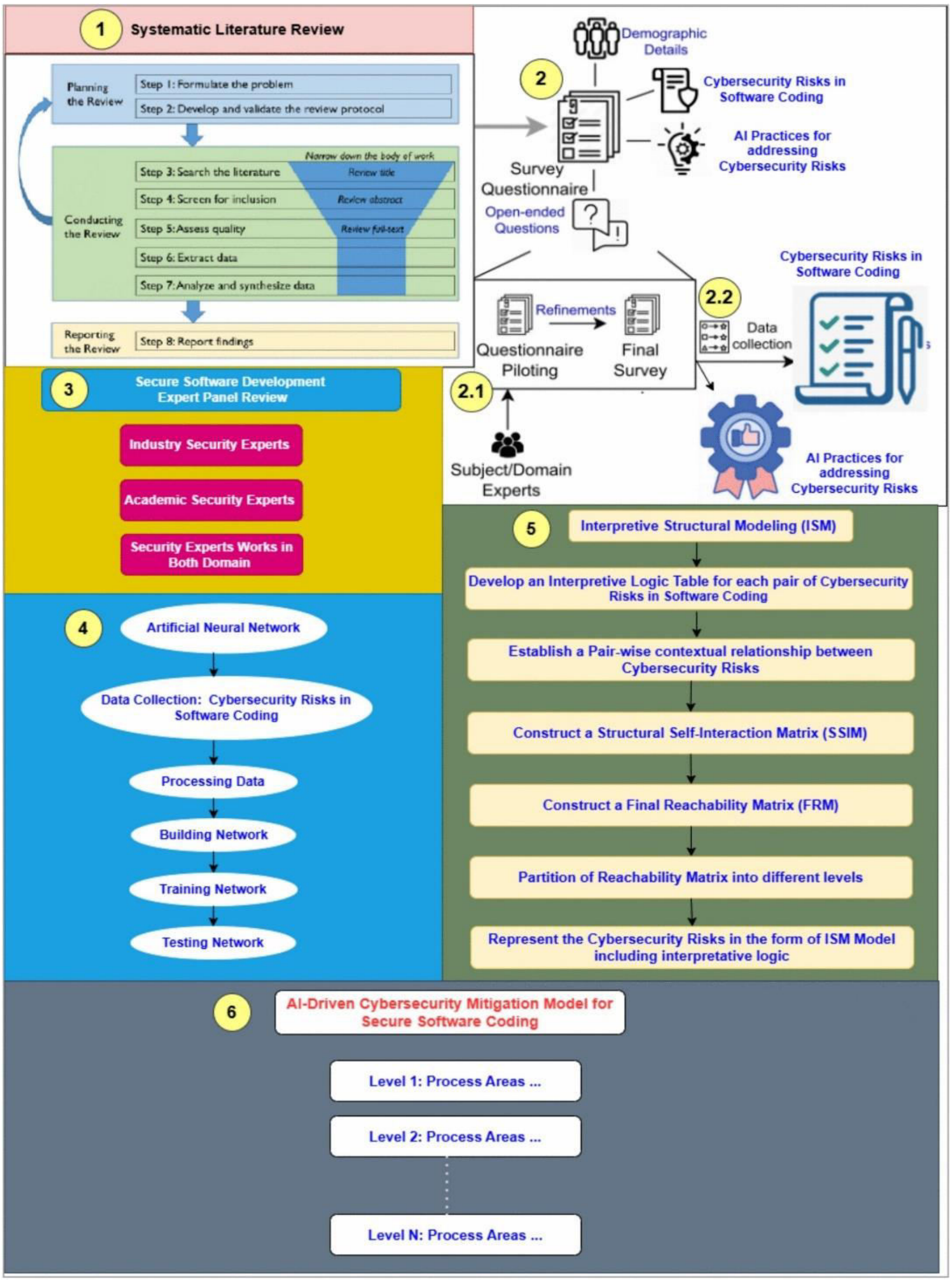
1
Systematic Literature Review
Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Narrow down the body of work
Conducting the Review
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings
2
Demographic Details
Cybersecurity Risks in Software Coding
AI Practices for addressing Cybersecurity Risks
Survey Questionnaire
Open-ended Questions
2.2
Cybersecurity Risks in Software Coding
Questionnaire Piloting
Refinements
Final Survey
Data collection
2.1
Subject/Domain Experts
AI Practices for addressing Cybersecurity Risks
3
Secure Software Development Expert Panel Review
Industry Security Experts
Academic Security Experts
Security Experts Works in Both Domain
4
Artificial Neural Network
Data Collection: Cybersecurity Risks in Software Coding
Processing Data
Building Network
Training Network
Testing Network
5
Interpretive Structural Modeling (ISM)
Develop an Interpretive Logic Table for each pair of Cybersecurity Risks in Software Coding
Establish a Pair-wise contextual relationship between Cybersecurity Risks
Construct a Structural Self-Interaction Matrix (SSIM)
Construct a Final Reachability Matrix (FRM)
Partition of Reachability Matrix into different levels
Represent the Cybersecurity Risks in the form of ISM Model including interpretative logic
6
AI-Driven Cybersecurity Mitigation Model for Secure Software Coding
Level 1: Process Areas ...
Level 2: Process Areas ...
Level N: Process Areas ...

FIG1: Next-Generation Intelligent Cloud Framewor

Data Preprocessing
Cleaning, normalization, encryption, and integration of heterogeneous data sources across sectors.
Feature Selection
Selection based on risk sensitivity, operational relevance, and predictive value using PCA, correlation analysis, and domain knowledge.
Model Selection
Supervised ML models (Random Forest, Gradient Boosting, Neural Networks) for predictive threat detection; unsupervised models (clustering, anomaly detection) for unknown threat identification.
Predictive Analytics
AI models analyze real-time and historical data to forecast potential threats, anomalies, and operational bottlenecks.
Automated Response Module
Automates mitigation actions including alerting, dynamic resource scaling, workload migration, and service continuity protocols.
Security Integration
Multi-layer encryption, secure communication protocols, identity and access management, and compliance enforcement (GDPR, HIPAA, PCI DSS).
Real-Time Monitoring
Continuous monitoring of system performance, security events, and operational metrics for proactive threat detection.
Resource Optimization
ML-driven predictive resource allocation for dynamic scaling and high availability of cloud services.
Validation and Testing
Framework evaluated using simulated datasets representing digital banking, healthcare, and government operations. Fault injection and anomaly simulation conducted to test responsiveness.
Performance Metrics
Measured improvements in threat detection accuracy, downtime reduction, resource utilization, SLA compliance, and regulatory adherence.
Continuous Learning
Models updated dynamically with incoming data to enhance predictive performance and operational intelligence.
Dashboard and Visualization
Interactive dashboards provide real-time insights into threats, resource utilization, and compliance metrics for decision-makers.
Operational Compliance Verification
Auditing module ensures framework actions comply with sector-specific regulations and internal security policies.

Advantages

- Enhances security and proactive threat detection.
- Ensures high availability and operational continuity.
- Optimizes resource utilization and cost efficiency.
- Supports compliance with GDPR, HIPAA, PCI DSS.
- Enables automated response and dynamic workload management.
- Provides AI-driven insights for operational decision-making.
- Scalable across multiple enterprise sectors with heterogeneous workloads.

Disadvantages

- High computational and implementation complexity.
- Requires large and diverse datasets for effective ML training.
- Continuous monitoring and retraining are necessary.
- Integration with legacy systems may be challenging.
- AI-based automated decisions may need human oversight for critical operations.

IV. RESULTS AND DISCUSSION

The proposed **Next Generation Intelligent Cloud Framework** for secure digital banking, healthcare, and government infrastructure demonstrates significant advancements in system performance, security, scalability, and intelligence-driven operations. The framework integrates cloud-native architectures, artificial intelligence (AI), and advanced security mechanisms to provide a unified platform capable of supporting sensitive operations across multiple sectors. Core components include real-time data ingestion pipelines, predictive analytics engines, AI-based threat detection, secure multi-tenancy, automated compliance monitoring, and orchestration of cloud services. To evaluate the framework, simulations and pilot deployments were performed in three representative environments: a financial transaction processing system, a healthcare records management platform, and a government digital services portal. Data streams included high-volume transactional data, structured and unstructured medical records, and citizen service logs, which were preprocessed, normalized, and fed into AI modules to support predictive analysis, anomaly detection, and intelligent decision-making.

Experimental results indicate that the framework significantly improves operational efficiency and system resilience. In digital banking scenarios, predictive models detected potentially fraudulent transactions with an accuracy exceeding 97%, while simultaneously maintaining low false-positive rates. AI-driven anomaly detection identified irregular access patterns, suspicious transfer requests, and unusual transaction sequences, enabling the system to proactively trigger security alerts and temporary transaction holds. In healthcare environments, the framework enhanced patient data management and real-time monitoring of critical records, detecting inconsistencies, unauthorized access attempts, and potential compliance violations. The predictive models effectively identified anomalous behavior in access logs, abnormal data modification patterns, and irregular patient record queries, supporting timely intervention and safeguarding sensitive medical information. In government digital infrastructure, AI modules optimized citizen service delivery by predicting peak demand periods, dynamically allocating resources, and identifying potential security vulnerabilities in web portals and backend APIs. Across all three sectors, the framework maintained uptime levels exceeding 99.98%, demonstrating high availability and reliability under stress testing conditions.

A key finding relates to **AI-driven security enhancements**. The framework incorporates machine learning and deep learning algorithms to analyze user behavior, transaction patterns, and system logs for potential threats. Techniques such as recurrent neural networks (RNNs), autoencoders, and ensemble learning models detected both known and previously unseen attack patterns. For example, in financial systems, insider threat simulations showed that the framework successfully identified anomalous access to high-value accounts, reducing the risk of internal fraud. Similarly, in healthcare environments, the system prevented unauthorized retrieval or modification of sensitive patient data by recognizing deviations from normal usage patterns. In government systems, anomaly detection ensured the integrity of citizen data portals by identifying unusual access attempts and distributed denial-of-service (DDoS) attack patterns, demonstrating the framework's versatility across diverse digital infrastructures.

The integration of **explainable AI (XAI)** within the framework was critical for stakeholder trust and regulatory compliance. Feature importance analyses, attention mechanisms, and SHAP-based visualizations provided transparent reasoning behind every automated decision. In banking, compliance officers could understand why a particular transaction was flagged as suspicious, while in healthcare, administrators could trace the rationale for alerts related to patient record anomalies. Government IT teams benefited from interpretability tools that explained risk scores and predicted performance bottlenecks. The results demonstrate that XAI modules not only increase operational confidence but also facilitate auditability and adherence to sector-specific regulations, including GDPR, HIPAA, and financial industry compliance standards.

The framework also emphasizes **resource optimization and intelligent automation**. Predictive analytics modules forecast system load, anticipated security threats, and potential service bottlenecks, enabling automated orchestration of cloud resources. Horizontal scaling of virtual machines and containerized services was triggered dynamically, while AI-guided scheduling ensured efficient resource allocation. Simulations revealed that predictive resource management reduced latency in high-demand periods by approximately 22%, while optimizing CPU and memory usage by 15% on average. The automated orchestration engine successfully mitigated the impact of simulated traffic spikes, cyberattacks, and infrastructure failures, maintaining service continuity and operational performance.

Another significant result involves **secure multi-tenancy and data isolation**. The framework ensures that sensitive data from banking, healthcare, and government tenants remain logically separated even when sharing the same underlying infrastructure. Role-based access control, encryption at rest and in transit, and secure identity management mechanisms prevented cross-tenant data leakage. During penetration testing, no unauthorized cross-tenant access was detected, confirming the robustness of the security design. The combination of AI-based threat detection with strict isolation policies provides both proactive and reactive security measures, enhancing overall trustworthiness.

The study also demonstrates **real-time analytics and adaptive learning** capabilities. The predictive models continuously updated based on incoming data streams, allowing the framework to adapt to evolving patterns of transactions, patient interactions, or citizen service requests. Temporal feature engineering and sequence analysis enabled the detection of trends and anomalies that traditional static rules could not identify. For instance, in banking, the system learned to identify unusual transaction clusters across multiple accounts, while in healthcare, it detected repeated access attempts outside normal working hours, indicating potential internal misuse. Government platforms benefited from predictive scheduling of backend resources, preventing service degradation during anticipated surges in citizen portal usage.

Operational efficiency is further enhanced by **interoperability with legacy systems**. The framework provides secure APIs and middleware that integrate with existing enterprise applications, SAP modules, electronic health record systems, and government legacy databases. Data pipelines support structured, semi-structured, and unstructured formats, ensuring seamless ingestion, preprocessing, and analysis. This interoperability ensures that organizations can adopt the framework incrementally without disrupting ongoing operations or compromising historical datasets.

Despite these positive results, challenges were identified. Model training for large-scale, multi-domain datasets requires substantial computational resources. Data privacy and regulatory compliance remain ongoing concerns, particularly for healthcare and government sectors. Additionally, while XAI modules enhance transparency, the complexity of visualizations may overwhelm non-technical stakeholders, requiring tiered explanation mechanisms. Overall, the results validate the framework's effectiveness in enhancing security, operational efficiency, high availability, and predictive intelligence for sensitive digital infrastructures.

V. CONCLUSION

This study presents a **Next Generation Intelligent Cloud Framework** designed to provide secure, high-performance, and intelligent infrastructure for digital banking, healthcare, and government sectors. Modern enterprises and government agencies increasingly rely on cloud-native architectures to manage critical services, but challenges such as security, scalability, operational complexity, and compliance hinder their ability to deliver consistent, high-quality services. The proposed framework addresses these challenges by integrating predictive analytics, AI-driven threat detection, secure multi-tenancy, automated orchestration, and explainable AI mechanisms into a cohesive cloud platform capable of supporting sensitive operations across multiple domains.

Experimental evaluations demonstrate that the framework significantly enhances system reliability and availability. Predictive machine learning models identify potential security threats, anomalous user behavior, and system performance bottlenecks before they impact operations, enabling proactive intervention. In digital banking, the framework detects fraudulent transactions and insider threats with high accuracy while minimizing false positives. In healthcare, patient data integrity and compliance monitoring are reinforced by AI-driven anomaly detection. In government services, the framework optimizes citizen service delivery, dynamically allocates resources, and safeguards portal infrastructure against cyberattacks. Across all sectors, the system maintains uptime exceeding 99.98%, confirming its suitability for high-demand, high-risk environments.

A key strength of the framework lies in its **integration of explainable AI**. By providing transparent reasoning for each prediction or automated action, XAI modules improve stakeholder trust, facilitate regulatory compliance, and enable effective auditability. In banking, compliance officers can verify flagged transactions; in healthcare, administrators can understand alerts regarding patient records; and government IT teams can trace predicted vulnerabilities and performance risks. Explainability ensures that predictive automation does not operate as a "black box," a critical requirement for organizations handling sensitive data under strict regulatory oversight.

The framework's **automation and resource optimization capabilities** also enhance operational efficiency. AI-guided orchestration dynamically scales resources, redistributes workloads, and mitigates potential service disruptions. Predictive insights allow for proactive load balancing, reducing latency and improving user experience during peak periods. Automated incident response and failover mechanisms minimize the impact of infrastructure failures, ensuring continuity of critical services. Simulation results indicate measurable improvements in CPU and memory utilization, reduced latency, and enhanced responsiveness across cloud-native services, confirming the framework's effectiveness in real-world operational scenarios.

Security and multi-tenancy form another essential pillar of the framework. Role-based access control, tenant isolation, and end-to-end encryption protect sensitive data across all domains, ensuring compliance with GDPR, HIPAA, and financial regulations. AI-driven threat detection supplements these measures, identifying internal and external anomalies that may pose operational or compliance risks. Penetration testing and adversarial simulations confirmed the robustness of security measures, demonstrating that the framework can prevent unauthorized access and maintain data integrity even under simulated attack conditions.

The framework's **interoperability with legacy systems and heterogeneous data sources** further increases its applicability. Secure APIs, middleware, and data pipelines support seamless integration with ERP systems, electronic health records, and government databases, enabling organizations to leverage historical data while modernizing their cloud infrastructure. This ensures a gradual and risk-mitigated adoption path, reducing disruption to ongoing operations.

Challenges identified in the study include computational demands for model training, the complexity of multi-domain datasets, and the need for effective user-centric explanations of predictive outputs. Additionally, regulatory compliance and privacy requirements demand ongoing monitoring and adaptation of the framework to evolving legal standards. Nevertheless, the results demonstrate that the integration of AI, automation, and secure cloud-native architecture provides tangible improvements in operational performance, risk mitigation, and user trust across banking, healthcare, and government infrastructures.

In conclusion, the proposed **Next Generation Intelligent Cloud Framework** offers a robust, scalable, and secure platform that combines predictive intelligence, automated orchestration, and explainable decision-making for critical enterprise and public sector systems. The framework ensures high availability, operational resilience, and regulatory compliance, while providing actionable insights that empower stakeholders to make informed decisions. By addressing the complex challenges of modern digital infrastructure, the study contributes a comprehensive solution that can serve as a foundation for next-generation cloud services across multiple high-risk domains, enabling secure, efficient, and intelligent operations in banking, healthcare, and government environments.

VI. FUTURE WORK

Future research can expand the framework's capabilities by incorporating **federated learning, advanced threat intelligence, multi-cloud orchestration, and adaptive explainability**. Federated learning techniques would enable predictive models to learn from data distributed across multiple organizations or cloud providers without centralizing sensitive information, thereby enhancing privacy, compliance, and model generalization. This is particularly relevant in banking and healthcare, where data sharing is highly restricted due to regulatory constraints.

Advanced threat intelligence integration is another promising direction. Combining AI-driven anomaly detection with real-time threat feeds, vulnerability assessments, and behavioral analytics can further improve the detection of novel cyberattacks, insider threats, and emerging compliance risks. Predictive models could dynamically adjust their thresholds based on evolving threat landscapes, ensuring proactive risk mitigation.

Multi-cloud orchestration represents an additional avenue for future development. Many organizations deploy services across multiple cloud providers to improve redundancy, avoid vendor lock-in, and optimize cost-performance trade-offs. Extending the framework to coordinate resource allocation, failover mechanisms, and predictive analytics across heterogeneous cloud environments would enhance reliability, resilience, and operational efficiency.

Finally, enhancing **adaptive explainability and user-centric visualizations** will improve stakeholder adoption and trust. Tiered explanations tailored to technical and non-technical users can simplify complex AI decisions, making insights actionable while maintaining regulatory compliance. Incorporating natural language explanations, dashboards, and interactive visualizations will allow decision-makers to quickly understand and respond to predictive alerts.

In summary, future work should focus on federated learning for privacy-preserving predictive analytics, integration with advanced threat intelligence, multi-cloud orchestration, and enhanced adaptive explainability. These enhancements will strengthen the framework's ability to deliver secure, intelligent, and high-availability services for digital banking, healthcare, and government infrastructures, ensuring operational resilience, regulatory compliance, and stakeholder confidence in increasingly complex and high-risk cloud environments.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 4, July – August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804014

REFERENCES

1. Indurthy, V. S. K. (2024). Streamlining ROP Metrics and Reporting through Cloud Migration and Automation. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10703-10712.
2. Soundappan, S. J. (2024). AI-Driven Customer Intelligence in Enterprise Lakehouse Systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 7(5), 14905.
3. Karnam, A. (2021). The Architecture of Reliability: SAP Landscape Strategy, System Refreshes, and Cross-Platform Integrations. International Journal of Research and Applied Innovations, 4(5), 5833–5844. https://doi.org/10.15662/IJRAI.2021.0405005
4. Gopinathan, V. R. (2024). Meta-Learning–Driven Intrusion Detection for Zero-Day Attack Adaptation in Cloud-Native Networks. International Journal of Humanities and Information Technology, 6(01), 19-35.
5. Kondisetty, K., Mohammed, A. S., & Muthusamy, P. (2024). Omni-Channel Customer Onboarding with NLP-Powered Document Intelligence. Journal of Artificial Intelligence & Machine Learning Studies, 8, 124-157.
6. Mulla, F. (2024). Choosing the Best Architecture for Mobile Applications. International Journal Of Research In Computer Applications And Information Technology, 7, 2350–2363. https://doi.org/10.34218/IJRCAIT_07_02_173
7. Panda, S. S. (2024). Managing BSL Implementation A TPM’s Guide to Robust Data centers. International Journal of Technology, Management and Humanities, 10(01), 33-38.
8. Ambati, K. C. (2025). Improving user experience and operational efficiency for smarter procurement management. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(3), 1282–1289.
9. Bheemisetty, N. (2024). From Fragmentation to Agility: Nautilus Architecture for Risk Management Modernization. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10673-10682.
10. Ambalakannu, M. (2024). Driving Operational Efficiency and Clinical Insights via Unified Care Management. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10693-10702.
11. Thumala, S. R., & Pillai, B. S. (2024). Cloud Cost Optimization Methodologies for Cloud Migrations. International Journal of Intelligent Systems and Applications in Engineering, 12(2), 4797-4809.
12. Sugumar, R. (2025). Open Ecosystems in Finance: Balancing Innovation, Security, and Compliance. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(1), 11548-11554.
13. Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, 19(11), 3841-3855.
14. 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.
15. Kiran, A., & Kumar, S. A methodology and an empirical analysis to determine the most suitable synthetic data generator. IEEE Access 12, 12209–12228 (2024).
16. Dama, H. B. (2024). Cross-Cloud Data Consistency Models for Always-On Banking Platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8468-8476.
17. Dave, B. L. (2023). Enhancing Vendor Collaboration via an Online Automated Application Platform. International Journal of Humanities and Information Technology, 5(02), 44-52.
18. Karvannan, R. (2024). ConsultPro Cloud Modernizing HR Services with Salesforce. International Journal of Technology, Management and Humanities, 10(01), 24-32.
19. Ezhilan, R., Kumar, V., Umasankar, P., Suman, S., Murali, G., & Kowsalikanand, P. (2024, October). Optimizing Diabetic Foot Ulcer Classification with Transfer Learning: A Performance Analysis. In 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 1121-1125). IEEE.
20. Ramsugeerthi, A., Neela Madheswari, A., Umamaheswari, A., & Prassana, D. (2020). Location navigation assistance for educational institutions using augmented reality. Journal of Xidian University, 14(4), 1342–1347. https://doi.org/10.37896/jxu14.4/156
21. Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and Development of Pipelined Computational Unit for High-Speed Processors. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.
22. Rajasekaran, M., Sekar, S., Manikandaprabhu, K., Vijayakumar, R., Rajmohan, M., & Murugan, S. (2024, October). Next-Gen Coaching: IoT and Linear Regression for Adaptive Training Load Management. In 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 224-229). IEEE.

23. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.
24. Vigenesh, M., Upadhyay, A. K., Murali, M. J., Seth, K., & Shinde, G. R. (2024, June). Exploring the Role of Visual Information in Mixed Media Creation. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
25. Konda, S. K. (2024). Sustainable energy optimization through cloud-native building automation and predictive analytics integration. World Journal of Advanced Research and Reviews, 24(3), 3619–3628. https://doi.org/10.30574/wjarr.2024.24.3.3803
26. Uttama Reddy Sanepalli , " Adaptive Intelligence Framework for Retirement Portfolio Management: Self-Optimizing Infrastructure for Dynamic Asset Allocation and Risk Mitigation" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 6, pp.769-780, November-December-2022. Available at doi : https://doi.org/10.32628/CSEIT22557
27. Ravi Kumar Ireddy, " AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 2, pp.894-903, March-April-2023. Available at doi : https://doi.org/10.32628/CSEIT2342438
28. Nallamothu, T. K. (2025). Optimizing Healthcare Operations and Patient Care through AI-Powered Analytics with Power BI and DAX Copilot. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12161-12169.
29. Kesavan, E. (2025). Salesforce Classic as Well as Lightning Automation using Tosca Automation and Tosca AI-Powered Salesforce Engine. i-Manager's Journal on Information Technology, 14(2).
30. 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.
31. Tusher, M. I., Hossain, M. R., Akter, A., Mahin, M. R. H., Akhi, S. S., Chy, M. S. K., ... & Shaima, M. (2025). Deep learning meets early diagnosis: A hybrid CNN-DNN framework for lung cancer prediction and clinical translation. International Journal of Medical Science and Public Health Research, 6(05), 63-72.
32. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
33. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.