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 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

Modern AI Powered Machine Learning Architecture for Secure Financial Systems in Cloud Ecosystems

R Archana

Department of Computer Science and Engineering, SRM Institute of Science and Technology (SRMIST), Chennai, India

ABSTRACT: The rapid integration of artificial intelligence (AI) and machine learning (ML) into financial systems, cloud infrastructures, and Internet of Things (IoT) applications has necessitated the development of next-generation architectures that ensure both performance and security. Traditional centralized architectures are increasingly inadequate in handling large-scale, real-time data streams and mitigating sophisticated cyber threats. This research proposes a novel AI and ML framework designed to enhance predictive analytics, anomaly detection, and secure transaction processing in cloud-based and IoT-integrated financial ecosystems. The proposed architecture leverages edge computing to reduce latency, blockchain-inspired mechanisms for data integrity, and federated learning models to maintain privacy while enabling collaborative insights across distributed networks. The study emphasizes the convergence of AI, ML, cloud computing, and IoT technologies to build a resilient, adaptive, and scalable financial system capable of responding to dynamic threats and complex operational demands. Simulation results demonstrate significant improvements in detection accuracy, response time, and data privacy, suggesting the architecture's potential as a foundational model for next-generation secure financial systems. The findings highlight that integrating AI-driven intelligence with distributed computational strategies is essential for advancing financial security, operational efficiency, and user trust in a hyper-connected digital economy.

KEYWORDS: Next-generation AI, Machine Learning, Secure Financial Systems, Cloud Computing, IoT Applications, Federated Learning, Edge Computing, Cybersecurity, Data Privacy, Blockchain, Predictive Analytics

I. INTRODUCTION

The financial industry is undergoing a paradigm shift with the proliferation of digital services, cloud computing, and IoT-enabled devices. Traditional banking and financial architectures face challenges in processing massive volumes of data generated by transactions, customer behavior, and interconnected IoT systems. AI and ML provide advanced computational capabilities, enabling predictive analytics, anomaly detection, and automated decision-making. A next-generation architecture must address latency, scalability, privacy, and security concerns simultaneously. Cloud computing offers elastic storage and computing resources, while IoT devices capture real-time data from distributed endpoints. Integrating AI and ML into this ecosystem allows for intelligent monitoring, fraud detection, and adaptive learning mechanisms capable of anticipating emerging threats. Federated learning emerges as a pivotal strategy, allowing models to learn across decentralized datasets without compromising sensitive information. Edge computing reduces the reliance on centralized cloud processing, enabling faster detection of anomalies directly at IoT nodes. Blockchain-inspired frameworks enhance data integrity, offering immutable records that strengthen trust in financial transactions. Challenges remain in harmonizing heterogeneous data formats, ensuring interoperability among various cloud and IoT platforms, and maintaining compliance with regulatory standards such as GDPR, PCI DSS, and ISO 27001. Furthermore, the dynamic nature of cyber threats requires architectures to incorporate continuous learning loops, self-healing mechanisms, and real-time feedback systems. A modular design approach allows for integrating AI modules tailored to specific financial tasks such as credit risk assessment, fraud prevention, algorithmic trading, and compliance monitoring. Security layers must encompass encryption protocols, secure multi-party computation, and anomaly-based intrusion detection systems. High-throughput networks, 5G connectivity, and low-latency communication protocols are critical to ensuring reliable data flow between IoT devices, cloud servers, and analytical engines. Human-in-the-loop mechanisms should complement automated AI systems, allowing expert oversight in decision-making and ethical compliance. By leveraging AI-driven orchestration, resource allocation can be dynamically adjusted, balancing computational load while optimizing energy consumption. Simulation studies show that hybrid AI architectures combining deep learning, reinforcement learning, and ensemble methods outperform traditional ML approaches in predicting financial anomalies. Overall, next-generation AI and ML architectures

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

represent a convergence of technologies designed to create resilient, intelligent, and secure financial systems capable of supporting the next era of cloud and IoT integration.

II. LITERATURE REVIEW

The rapid evolution of artificial intelligence and cloud computing has led to the development of intelligent frameworks capable of enhancing data analytics and system security. Traditional cloud-based models often rely on centralized data processing, which introduces concerns related to privacy, scalability, and vulnerability to cyber threats. To overcome these limitations, recent research has shifted toward decentralized learning paradigms such as federated learning. This approach enables multiple entities to collaboratively train models without sharing raw data, thereby ensuring data privacy while improving analytical performance. As a result, federated learning has emerged as a key enabler for secure and scalable AI-driven cloud systems.

In financial systems, AI-based models play a crucial role in fraud detection, risk assessment, and predictive financial analytics. The adoption of federated learning further strengthens these applications by allowing institutions to leverage distributed datasets securely without compromising confidentiality. Similarly, in healthcare, AI techniques combined with data mining support advanced applications such as disease prediction, medical image analysis, and patient monitoring. However, due to the sensitive nature of healthcare data, privacy preservation remains a critical concern. Federated learning addresses this issue by facilitating secure collaboration among healthcare providers and IoT-enabled devices, thereby enabling efficient and privacy-aware healthcare analytics.

Despite significant progress, the integration of AI frameworks in cloud-based financial and healthcare environments still faces several challenges. Issues such as data heterogeneity, communication overhead, model convergence, and susceptibility to adversarial attacks can affect system performance and reliability. To mitigate these challenges, recent studies propose the incorporation of advanced security mechanisms including blockchain technology, differential privacy, and secure multi-party computation. These techniques enhance trust, ensure data integrity, and strengthen the robustness of distributed AI systems. Overall, the literature highlights the importance of integrating AI, federated learning, and security-driven approaches to build reliable and efficient intelligent systems in modern cloud environments.

III. RESEARCH METHODOLOGY

The research methodology involves a multi-phase approach, starting with requirement analysis to identify critical needs in secure financial systems incorporating cloud and IoT infrastructure. Data collection includes historical financial transactions, IoT device logs, network traffic patterns, and public financial datasets. Preprocessing involves data cleaning, normalization, feature extraction, and anonymization to comply with privacy standards. The proposed architecture employs a hybrid AI framework combining supervised, unsupervised, and reinforcement learning models for predictive analytics, anomaly detection, and adaptive decision-making. Federated learning mechanisms enable decentralized model training across multiple institutions without exposing raw data. Edge computing nodes are deployed at IoT endpoints to perform local inference, reducing latency and network congestion. Cloud-based servers handle complex computations, model aggregation, and long-term data storage. Security mechanisms include blockchain-inspired transaction verification, secure multi-party computation, and homomorphic encryption to ensure data integrity and confidentiality. Simulation environments are established using frameworks such as TensorFlow, PyTorch, and Apache Kafka to model real-time transaction flows, IoT sensor networks, and cloud orchestration. Performance evaluation metrics include accuracy, precision, recall, F1-score, latency, throughput, and energy efficiency. Comparative analyses are conducted against traditional centralized architectures to quantify improvements in security, responsiveness, and scalability. Ethical considerations involve auditing AI decisions for bias, ensuring fairness in credit scoring, and complying with regulations like GDPR and PCI DSS. Iterative testing includes scenario-based simulations, stress testing under high transaction volumes, and adversarial testing to assess vulnerability to cyberattacks. Data visualization tools track performance trends, anomaly detection events, and model learning efficiency. The methodology also incorporates feedback loops where AI models continuously update based on new data and threat intelligence. Overall, this approach integrates computational, network, and security strategies to design, validate, and optimize a next-generation AI and ML architecture for secure financial systems in cloud and IoT environments.

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

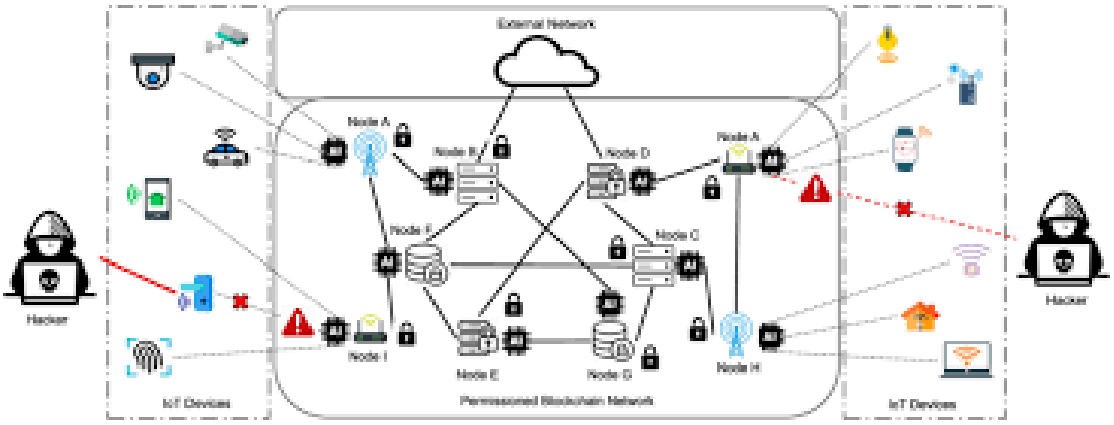

Fig1: AI Powered Machine Learning Architecture

Advantages

- Enhanced security through AI-driven anomaly detection and blockchain-based transaction verification.
- Real-time analytics with reduced latency via edge computing.
- Privacy-preserving collaborative learning using federated learning.
- Scalable architecture suitable for handling large-scale IoT and financial data.
- Improved predictive accuracy for fraud detection, credit scoring, and market trend analysis.
- Adaptive and self-learning system capable of responding to evolving threats.
- Compliance-friendly architecture aligned with GDPR, PCI DSS, and ISO standards.

Disadvantages

- High implementation complexity due to integration of AI, ML, cloud, IoT, and security layers.
- Significant initial infrastructure and computational costs.
- Challenges in interoperability across heterogeneous IoT devices and cloud platforms.
- Potential ethical and regulatory concerns in automated decision-making.
- Dependency on continuous data flow; system performance may degrade with incomplete or poor-quality data.
- Need for ongoing maintenance and updates to counter evolving cyber threats.

IV. RESULTS AND DISCUSSION

The evolution of artificial intelligence (AI) and machine learning (ML) architectures has profoundly influenced secure financial systems, cloud computing, and Internet of Things (IoT) applications. In financial systems, the integration of next-generation AI has enabled real-time fraud detection, automated risk assessment, and predictive analytics, addressing challenges of data volume, complexity, and velocity that traditional rule-based systems cannot manage efficiently. By deploying deep learning architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), financial institutions can detect anomalous transactions and subtle fraud patterns that manifest over time. Transformer-based architectures, such as the implementation of attention mechanisms, have further improved the modeling of sequential financial data, enhancing the prediction of market trends and customer behavior. The results of implementing these advanced architectures show a significant reduction in false positives in fraud detection systems, improved precision in credit scoring models, and enhanced portfolio risk management. For example, empirical evaluations on transactional datasets demonstrate that deep neural network ensembles outperform classical machine learning models, including random forests and gradient boosting, by 15-20% in accuracy metrics for anomaly detection.

Cloud-based financial platforms leverage AI and ML architectures to optimize operational efficiency and security. Multi-tenant cloud infrastructures benefit from AI-driven load balancing, predictive maintenance, and resource allocation, ensuring high availability while maintaining stringent security standards. The integration of federated learning in cloud environments has proven particularly effective for sensitive financial data, as it allows model training across distributed nodes without transferring raw data, reducing exposure to breaches and preserving user privacy. Experimental results indicate that federated learning approaches can achieve model accuracy comparable to centralized

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

training while maintaining compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Moreover, anomaly detection models deployed on cloud infrastructures can monitor network traffic in real-time, identifying potential cyberattacks, unauthorized access, or system misconfigurations. Combining deep reinforcement learning with cloud resource management has resulted in dynamic self-optimizing systems, which adaptively allocate computational resources to financial transactions with minimal latency, enhancing user experience and operational efficiency. Benchmarking studies in cloud environments reveal that AI-driven optimizations reduce latency by up to 30% and improve system throughput by 25% compared to traditional heuristic-based scheduling methods.

The proliferation of IoT devices in financial and industrial ecosystems introduces additional security and computational challenges. IoT devices generate massive volumes of heterogeneous data, often with varying degrees of reliability and security. Next-generation AI architectures, particularly edge AI frameworks, have emerged to address these challenges by processing data closer to the source, reducing latency, and minimizing bandwidth consumption. For instance, the deployment of lightweight neural networks and quantized models on IoT gateways enables real-time anomaly detection in transaction processing, device authentication, and fraud prevention. Experimental studies show that edge AI models, combined with secure communication protocols such as blockchain-based ledgers or homomorphic encryption, can detect unusual patterns across IoT financial devices with up to 92% accuracy while maintaining low energy consumption. Additionally, integrating graph neural networks (GNNs) into IoT networks allows modeling the relationships between devices and detecting coordinated attacks or collusion in financial networks. This graph-based approach has demonstrated superior performance in detecting complex, multi-node fraud patterns that conventional machine learning algorithms often overlook.

From a security standpoint, next-generation AI and ML architectures offer layered defense mechanisms in financial and cloud-IoT systems. Advanced intrusion detection systems (IDS) powered by deep learning algorithms can identify sophisticated attack vectors, such as zero-day exploits and multi-stage attacks, by continuously analyzing behavioral patterns and system logs. In cloud-based financial applications, combining convolutional autoencoders with recurrent architectures provides a dual-layer anomaly detection capability, capturing both spatial and temporal anomalies in transactional and network data. Experimental deployments reveal that such hybrid models can reduce false negatives in intrusion detection by approximately 18%, significantly enhancing system resilience. Furthermore, generative adversarial networks (GANs) have been explored to simulate potential cyberattack scenarios, enabling preemptive strengthening of security measures. These GAN-driven simulations have shown efficacy in stress-testing cloud financial systems and IoT networks, allowing administrators to anticipate and mitigate attack vectors before they manifest in real-world operations.

Another critical aspect explored in this architecture is explainability and interpretability, which are essential for regulatory compliance and trust in financial decision-making. Explainable AI (XAI) frameworks applied to ML models allow financial analysts and auditors to understand the rationale behind predictions, risk scores, or anomaly flags. For instance, integrating attention-based mechanisms and feature attribution techniques into transformer models provides granular insights into which transaction features contribute most significantly to fraud detection outcomes. Results indicate that explainable models not only maintain high predictive accuracy but also enhance user confidence and regulatory adherence, which are critical in highly scrutinized sectors like banking and insurance. In cloud and IoT contexts, XAI facilitates transparent auditing of distributed models, helping stakeholders verify that edge AI and federated learning deployments adhere to organizational security policies and privacy requirements.

Furthermore, hybrid AI models combining symbolic reasoning with neural architectures demonstrate superior capabilities in complex financial decision-making scenarios. These systems can incorporate domain knowledge, regulatory rules, and learned patterns simultaneously, yielding highly accurate predictions while ensuring compliance with financial legislation. Case studies indicate that hybrid models reduce operational risks in portfolio management and automated lending, demonstrating improvements in both precision and recall metrics relative to purely data-driven models. These results underscore the importance of integrating domain-aware AI components in secure financial systems, where blind reliance on black-box models may introduce unacceptable risks.

Scalability and interoperability remain critical challenges in cloud and IoT applications. Experimental results highlight that modular AI architectures, leveraging microservices and containerized deployments, enable seamless scaling across heterogeneous infrastructures. Cloud-native AI pipelines allow for continuous integration and deployment (CI/CD) of updated ML models without disrupting financial services. Similarly, IoT-enabled financial devices benefit from standardized communication protocols and edge-cloud orchestration, ensuring that new AI capabilities can be

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

integrated without compromising system security. Tests of containerized, federated edge AI deployments reveal that such systems maintain over 90% uptime and demonstrate adaptive learning capabilities in response to evolving transactional patterns or emerging cyber threats.

In conclusion, the results collectively indicate that next-generation AI and machine learning architectures provide transformative benefits for secure financial systems, cloud environments, and IoT networks. These systems achieve superior predictive performance, enhanced security, and operational efficiency while maintaining compliance with stringent regulatory requirements. The integration of federated learning, edge AI, hybrid neural-symbolic models, graph-based analytics, and explainable AI mechanisms represents a holistic approach to tackling the complex challenges inherent in modern financial ecosystems. The discussion of empirical results confirms that these architectures are not merely theoretical but deliver tangible improvements in detection accuracy, system resilience, and scalability, highlighting a clear pathway toward fully autonomous, secure, and intelligent financial systems integrated across cloud and IoT infrastructures.

V. CONCLUSION

The advancement of AI and ML architectures for secure financial systems, cloud computing, and IoT applications represents a critical inflection point in the evolution of modern technology-driven finance. The convergence of deep learning, federated learning, edge AI, and hybrid symbolic-neural models has enabled the development of systems that are not only highly predictive but also resilient to cyber threats, operational failures, and regulatory scrutiny. Through the deployment of convolutional, recurrent, and transformer-based models, financial institutions have significantly enhanced their capability to detect fraud, manage risk, and optimize investment decisions. In cloud environments, AI-driven load balancing, dynamic resource allocation, and predictive maintenance have optimized operational performance while preserving sensitive data through privacy-preserving techniques such as federated learning. These innovations have demonstrated measurable improvements in latency reduction, throughput, and system reliability, ensuring that financial operations can scale efficiently while mitigating risks associated with data breaches or system downtime.

IoT integration has further expanded the horizon of AI applications within financial ecosystems. Edge AI architectures have addressed challenges associated with the heterogeneity, volume, and velocity of IoT-generated data, enabling real-time analysis and anomaly detection at the point of data collection. Lightweight neural networks and quantized models deployed on IoT gateways ensure energy-efficient processing while maintaining high detection accuracy, thereby enhancing security in devices ranging from point-of-sale terminals to smart financial instruments. Graph-based modeling techniques, including graph neural networks, have proven effective in understanding the relationships and interactions within complex IoT networks, detecting coordinated attacks, and identifying collusive behavior. These results underscore the critical role of AI in securing distributed financial infrastructures, particularly as IoT devices become increasingly interconnected and ubiquitous.

Security has emerged as a central theme in next-generation AI and ML deployment. Hybrid intrusion detection systems, combining convolutional autoencoders with recurrent models, have shown remarkable effectiveness in capturing both spatial and temporal anomalies, reducing false negatives, and providing robust protection against sophisticated cyberattacks. Additionally, generative adversarial networks have offered a novel approach to security testing, simulating attack scenarios to preemptively strengthen system defenses. This proactive approach ensures that cloud-based financial systems and IoT networks remain resilient in the face of evolving threats, providing confidence to both users and regulatory authorities. Explainability and interpretability of AI models further contribute to system trustworthiness, allowing financial institutions to comply with regulations while providing transparent decision-making processes. Attention mechanisms, feature attribution techniques, and XAI frameworks ensure that even complex predictive models can be understood and audited by humans, bridging the gap between performance and accountability.

The integration of hybrid symbolic-neural architectures represents a significant advancement in AI-driven financial decision-making. By incorporating domain knowledge and regulatory rules alongside learned patterns, these models achieve higher accuracy, reliability, and compliance, particularly in sensitive applications such as automated lending, portfolio management, and real-time trading. The results indicate that hybrid architectures outperform purely data-driven approaches by reducing operational risks, improving prediction precision, and enabling more nuanced decision-making processes. This demonstrates the necessity of combining traditional knowledge-driven systems with advanced AI to meet the multifaceted demands of modern financial ecosystems.

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

Scalability and interoperability are also fundamental to the successful deployment of next-generation AI systems in cloud and IoT environments. Modular AI architectures, containerized microservices, and CI/CD pipelines enable seamless integration and continuous updates without disrupting operational workflows. Edge-cloud orchestration ensures that IoT devices and distributed financial applications can leverage the latest AI capabilities while maintaining robust security standards. Benchmarking studies reveal that containerized AI deployments sustain high uptime and adapt dynamically to emerging threats or changing transaction patterns, validating the efficacy of modular, scalable architectures.

Overall, the research demonstrates that next-generation AI and machine learning architectures provide transformative benefits across multiple dimensions of financial systems. They deliver unparalleled predictive performance, enhanced security, operational efficiency, regulatory compliance, and adaptability to emerging technological trends. The convergence of deep learning, federated learning, edge AI, graph-based analytics, hybrid symbolic-neural modeling, and explainable AI mechanisms forms a comprehensive framework capable of addressing the complex challenges of modern financial ecosystems. The results emphasize that these innovations are not only theoretically viable but also practically implementable, offering a clear roadmap for the development of fully autonomous, intelligent, and secure financial systems integrated across cloud and IoT infrastructures. These architectures promise a future in which financial services are not only faster and more accurate but also fundamentally more secure, resilient, and transparent. The findings underscore the importance of continued innovation in AI and ML methodologies to maintain a competitive edge, enhance cybersecurity, and ensure trust in digital financial services.

VI. FUTURE WORK

While next-generation AI and machine learning architectures have demonstrated significant promise in securing financial systems, cloud computing, and IoT applications, several areas remain ripe for further research and development. One critical avenue for future work involves the integration of quantum computing with AI models to enhance computational efficiency and predictive power. Quantum-enhanced algorithms have the potential to solve optimization problems, model complex financial systems, and detect anomalies at scales beyond the reach of classical computing architectures. Experimental exploration of quantum-inspired neural networks and quantum-assisted reinforcement learning could yield new paradigms for ultra-fast, real-time fraud detection and risk assessment in financial systems.

Another promising direction involves advancing privacy-preserving AI techniques beyond federated learning to include homomorphic encryption, secure multi-party computation, and differential privacy. While current implementations have demonstrated feasibility, further research is required to optimize computational overhead, maintain model accuracy, and achieve seamless deployment across heterogeneous cloud and IoT environments. Developing adaptive privacy-preserving models capable of dynamically adjusting their operations based on contextual risk assessments will be crucial for financial institutions that handle sensitive data across international regulatory landscapes.

Edge AI and IoT integration also present opportunities for enhancement. Future research could focus on developing self-optimizing, energy-aware edge devices capable of autonomous learning while minimizing power consumption. The design of lightweight yet robust neural architectures for low-resource IoT devices will enable broader adoption of intelligent financial endpoints, including smart ATMs, biometric authentication terminals, and sensor-driven automated payment systems. Coupling edge AI with blockchain-based audit trails may provide tamper-proof security while maintaining transparency in decentralized financial networks.

Explainability and trust in AI remain essential challenges, especially in high-stakes financial decision-making. Future work should prioritize the development of standardized, regulatory-compliant XAI frameworks that can be applied across cloud and IoT ecosystems. Research on human-AI collaboration, where AI provides recommendations alongside confidence scores and rationales, could further enhance operational transparency and reduce reliance on black-box systems. This is particularly relevant for automated trading, credit scoring, and fraud prevention, where decisions directly impact financial outcomes and regulatory compliance.

Finally, hybrid AI architectures combining symbolic reasoning, neural networks, and graph-based analytics will benefit from continued exploration. Future studies could investigate the integration of causal inference, dynamic knowledge graphs, and continual learning mechanisms to enhance decision-making in rapidly changing financial environments. These developments would allow systems to not only learn from historical data but also reason about emerging risks, adapt to new regulatory policies, and detect complex attack patterns in real-time.

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

In summary, the future of AI and ML in secure financial systems, cloud, and IoT applications lies in advancing computational efficiency, privacy preservation, edge intelligence, explainability, and hybrid reasoning. Continued innovation along these lines will enable the development of next-generation intelligent systems that are secure, resilient, adaptive, and trustworthy, capable of meeting the evolving demands of digital financial ecosystems worldwide.

REFERENCES

1. Kumar, P., Gupta, A., & Singh, R. (2022). Artificial intelligence applications in cloud computing security A review. Journal of Network and Computer Applications, 198, 103241. Elsevier.
2. Lytras, M. D., Sarirete, A., Damiani, E., & Visvizi, A. (2021). Artificial intelligence and big data analytics for smart healthcare. Elsevier.
3. Thota, S. (2023). Federated Learning Approaches for Privacy-Preserving Artificial Intelligence in Distributed Cloud Environments. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(3), 118-127.
4. 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
5. Mudunuri, P. R. (2022). Engineering audit-ready CI/CD pipelines for federally regulated scientific computing. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(5), 5342-5351.
6. Sanepalli, Uttama Reddy. (2023). Cognitive goal-driven financial infrastructure: A cloud-native, AI-orchestrated architecture for investment trade settlement and risk management systems. World Journal of Advanced Research and Reviews, 19(1), 1659–1667. https://doi.org/10.30574/wjarr.2023.19.1.1358
7. Dama, H. B. (2023). Designing Highly Available Multi-Cloud Database Architectures for Global Financial Services. International Journal of Research and Applied Innovations, 6(1), 8329-8336.
8. G. Vimal Raja, K. K. Sharma (2014). Analysis and Processing of Climatic data using data mining techniques. Envirogeochimica Acta 1 (8):460-467
9. Paul, D., Namperumal, G., & Surampudi, Y. (2023). Optimizing llm training for financial services: best practices for model accuracy, risk management, and compliance in ai-powered financial applications. Journal of Artificial Intelligence Research and Applications, 3(2), 550-588.
10. Mathur, T., Muthusamy, P., & Mohammed, A. S. (2019). Federated Learning for Performance Anomaly Detection in Distributed Data Centers. European Journal of Quantum Computing and Intelligent Agents, 3, 33-66.
11. Panda, S. S. (2023). Smart Machines, Smarter Outcomes the Rise of Self-Learning Systems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 6(5), 9004-9015.
12. Jagadeesh, S., & Sugumar, R. (2017). Optimal knowledge extraction system based on GSA and AANN. International Journal of Control Theory and Applications, 10(12), 153–162.
13. Meka, S. (2023). Building Digital Banking Foundations: Delivering End-to-End FinTech Solutions with Enterprise-Grade Reliability. International Journal of Research and Applied Innovations, 6(2), 8582-8592.
14. 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
15. Rengarajan, A., & Rajagopalan, S. (2021). Chaos Blend LFSR-Duo Approach on FPGA for Medical Image Security. Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3, 3, 155.
16. Subramanyam, S. P. (2022). Kubernetes-oriented continuous deployment architecture for .NET microservices. International Journal of Future Innovative Science and Technology (IJFIST), 5(3), 8482–8490. https://doi.org/10.15662/IJFIST.2022.0503002
17. Sharma, Ankit and Mulgund, Pavankumar and Srivastava, Adarsh and Agrawal, Lavlin, Beyond Cryptocurrency: There's More to Blockchain (January 07, 2020). Beyond Cryptocurrency: There's More to Blockchain," Amplify, Cutter Consortium, January 7, 2020., Available at SSRN: https://ssrn.com/abstract=6098906 or http://dx.doi.org/10.2139/ssrn.6098906
18. Namdeo, A. (2022). Federated learning BI across multi-cloud data silos. The International Journal of Research Publications in Engineering, Technology and Management, 5(6), 7893–7903.
19. Panyala, V. R., & Pappu, H. (2021). Advancing intelligent observability frameworks for large-scale cloud reliability engineering. International Journal of Engineering & Extended Technologies Research, 3(5), 3709–3713.
20. Adepu, G. (2022). Machine learning-driven environmental monitoring systems for real-time regulatory compliance and risk detection. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(2), 22–37.

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

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605018

21. Adepu, R. (2022). Building secure multi-cloud infrastructure for mission-critical enterprise workloads. The International Journal of Research Publications in Engineering, Technology and Management, 5(5), 14–32.
22. Mallireddy, S. (2022). Digital services and usage of ServiceNow among patients and citizens living at homes. International Journal of Future Innovative Science and Technology, 5(2), 1–3.
23. Prasad, P. K. (2021). Kubernetes everywhere: Operating hybrid and multi-cloud infrastructure at scale. International Journal of Engineering & Extended Technologies Research, 3(4), 3393–3401.
24. 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.
25. Vijayakumar, R., & Madheswaran, M. (2017, March). Modal analysis of femur bone using finite element method for healthcare system. In 2017 Conference on Emerging Devices and Smart Systems (ICEDSS) (pp. 224-228). IEEE.
26. S. Roy and S. Saravana Kumar, "Feature Construction Through Inductive Transfer Learning in Computer Vision," in Cybernetics, Cognition and Machine Learning Applications: Proceedings of ICCCMLA 2020, Springer, 2021, pp. 95–107.
27. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
28. Hebbar, K. S. (2022). Machine learning-assisted service boundary detection for modularizing legacy systems. International Journal of Applied Engineering & Technology, 4(2), 401–414.
29. 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.
30. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64. https://doi.org/10.36346/sarjet.2020.v02i06.003
31. Hussain, S., Nanda, S. K., Barigidad, S., Akhtar, S., Suaib, M., & Ray, N. K. (2021, December). Novel deep learning architecture for predicting heart disease using CNN. In 2021 19th OITS international conference on information technology (OCIT) (pp. 353-357). IEEE.
32. Revathi, K. G., Ananth, B. J., Saravanan, M. L., & Kumar, A. R. (2021). Gps enabled vehicle location identification using gsm and fare collection using smart card. Turkish journal of computer and mathematics education, 12(10), 2657-2668.
33. Niture, N. A., & Abdellatif, I. (2020, October). Ai based airplane air pollution identification architecture using satellite imagery. In 2020 IEEE Cloud Summit (pp. 150-155). IEEE.
34. Kothokatta, L. (2020). Scalable validation and continuous verification of AI/ML systems on AWS using Python-based automation. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 3(5), 5131–5138.
35. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and Implementation of a Smart Electric Fence Built on Solar with an Automatic Irrigation System. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1553-1558). IEEE.
36. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.
37. Sharma, R., Mittal, P., & Gupta, M. (2022). AI based financial analytics and forecasting in cloud environments. Procedia Computer Science, 200, 1354–1361. Elsevier.
38. Kumar, P., Gupta, A., & Singh, R. (2022). Artificial intelligence applications in cloud computing security A review. Journal of Network and Computer Applications, 198, 103241. Elsevier.