International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

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

DOI: 10.15680/IJCTECE.2025.0806029

Zero Trust AI-Powered Cybersecurity Framework for Cloud-Native Banking, Healthcare, and Government Systems

Johan Fabry

Senior Technical Team Lead, United Kingdom

ABSTRACT: The rapid digital transformation across banking, healthcare, and government sectors has significantly increased the reliance on cloud-native systems for storing, processing, and transmitting sensitive data. However, this transition has also expanded the attack surface, making these sectors prime targets for sophisticated cyber threats. Traditional perimeter-based security models are no longer sufficient to protect distributed and dynamic cloud environments. This paper proposes a **Zero Trust AI-powered cybersecurity framework** designed to secure cloud-native infrastructures used in critical sectors such as banking, healthcare, and government systems. The framework integrates Zero Trust principles, artificial intelligence–based threat detection, identity-centric security controls, and continuous monitoring mechanisms. By combining AI-driven analytics with strict access verification and automated threat response, the proposed framework strengthens data protection, improves real-time threat detection, and enhances resilience against advanced cyberattacks. The model ensures that every user, device, and application is continuously verified before accessing resources, thereby minimizing the risk of unauthorized access and data breaches.

KEYWORDS: Zero Trust security, AI-powered cybersecurity, Cloud-native security, Banking cybersecurity, Healthcare data protection, Government cybersecurity, Machine learning security, Continuous authentication, Threat detection, Cloud infrastructure security

I. INTRODUCTION

In recent years, cloud computing and cloud-native architectures have revolutionized how organizations deploy applications and manage data. Critical sectors such as banking, healthcare, and government services increasingly rely on digital infrastructures to deliver services efficiently and securely. Banking systems manage financial transactions and sensitive customer information, healthcare systems store electronic health records and patient data, and government systems handle confidential national and citizen data. As these sectors adopt cloud-native technologies, ensuring robust cybersecurity becomes a critical requirement.

Traditional cybersecurity approaches were designed around perimeter-based security models, where internal networks were considered trusted while external networks were considered untrusted. However, the modern digital environment includes remote work, mobile devices, third-party integrations, and multi-cloud platforms. These changes have weakened the traditional network perimeter and created new vulnerabilities that attackers can exploit.

The **Zero Trust security model** has emerged as an effective approach for securing modern IT infrastructures. Instead of assuming trust based on network location, Zero Trust requires continuous verification of every access request, regardless of whether it originates from inside or outside the network. Every user, device, and application must authenticate and prove authorization before accessing resources.

Artificial Intelligence (AI) further enhances cybersecurity by enabling intelligent threat detection and automated response mechanisms. AI algorithms can analyze vast amounts of security data, detect anomalies, and identify patterns associated with cyber threats. Integrating AI with Zero Trust security principles provides a powerful framework for protecting cloud-native environments in high-risk sectors.

This paper presents a **Zero Trust AI-powered cybersecurity framework** designed to secure cloud-native banking, healthcare, and government systems. The framework combines identity-based access control, continuous

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

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

DOI: 10.15680/IJCTECE.2025.0806029

authentication, behavioral analytics, and automated threat response to create a resilient security architecture capable of defending against modern cyber threats.

II. LITERATURE REVIEW

The rapid digital transformation of critical sectors such as banking, healthcare, and government has significantly increased the reliance on cloud-native infrastructures. While cloud technologies provide scalability, flexibility, and cost efficiency, they also introduce new cybersecurity challenges due to distributed architectures and complex system integrations. Researchers have emphasized the importance of adopting advanced security frameworks to protect sensitive data and critical infrastructure from sophisticated cyber threats.

Traditional cybersecurity models were primarily based on **perimeter-based security**, where systems inside the network were considered trusted and external entities were treated as untrusted. However, with the growth of cloud computing, remote access, mobile devices, and third-party integrations, the network boundary has become less defined. Studies have shown that perimeter-based models are insufficient for protecting modern distributed systems, particularly in sectors that handle sensitive information such as financial records, medical data, and government databases.

The **Zero Trust security model** has emerged as a promising solution for addressing these challenges. Zero Trust architecture is based on the principle of "never trust, always verify," meaning that every user, device, and application must be authenticated and authorized before accessing resources. Researchers have demonstrated that Zero Trust frameworks improve security by implementing continuous authentication, strict access control policies, and real-time monitoring of user behavior. This approach is particularly beneficial for cloud-native systems where resources are dynamically accessed from multiple locations and devices.

In recent years, **Artificial Intelligence (AI) and Machine Learning (ML)** have been increasingly integrated into cybersecurity systems. AI-based security solutions can analyze large volumes of security data, detect anomalies, and identify potential cyber threats in real time. Machine learning algorithms are widely used in intrusion detection systems, malware analysis, fraud detection, and behavioral analytics. Studies indicate that AI-driven threat detection systems can significantly improve detection accuracy and reduce response time compared to traditional rule-based systems.

Several research studies have also explored the application of AI-driven cybersecurity in **sector-specific environments**. In the banking sector, AI-based systems are used to detect fraudulent transactions, monitor financial activities, and prevent unauthorized access to financial platforms. In healthcare systems, AI-driven security tools help protect electronic health records and ensure secure access to patient data. Government institutions have also adopted AI-based cybersecurity solutions to protect national infrastructure, citizen information, and confidential governmental data from cyber espionage and advanced persistent threats.

Despite these advancements, existing research highlights several challenges associated with implementing AI-powered cybersecurity frameworks. These challenges include data privacy concerns, model transparency issues, and the complexity of integrating AI systems into existing enterprise infrastructures. Additionally, maintaining regulatory compliance and ensuring secure data sharing across multiple cloud environments remain significant concerns for organizations in critical sectors.

Overall, the literature indicates that combining **Zero Trust security principles with AI-driven threat detection** provides a strong foundation for protecting cloud-native infrastructures. This integrated approach enhances identity verification, enables continuous monitoring, and supports automated threat response mechanisms. The proposed research builds upon these concepts by developing a comprehensive Zero Trust AI-powered cybersecurity framework designed specifically for cloud-native banking, healthcare, and government systems.

III. METHODOLOGY

The methodology for developing the proposed cybersecurity framework follows a structured approach consisting of system design, data collection, AI model development, Zero Trust implementation, and performance evaluation.

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

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

DOI: 10.15680/IJCTECE.2025.0806029

The first stage involves **architecture design** for cloud-native environments. The proposed system uses containerized applications and microservices deployed on scalable cloud platforms. Security is integrated at every layer of the architecture, including identity management, network segmentation, encrypted data storage, and secure APIs. A Zero Trust access control model ensures that no entity is automatically trusted, and all access requests must undergo verification.

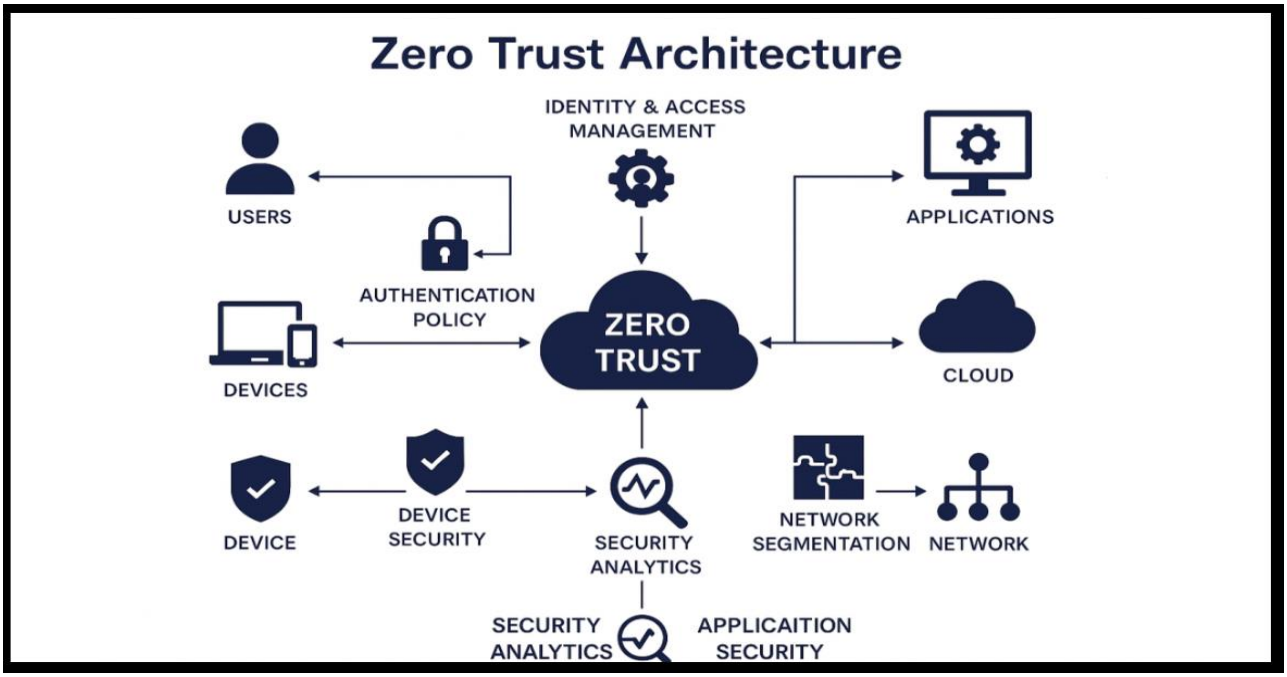

Figure 1: Zero Trust AI-Powered Cybersecurity Framework for Cloud-Native Banking, Healthcare, and Government Systems

The figure illustrates a **Zero Trust AI-Powered Cybersecurity Framework** designed to protect cloud-native digital infrastructures used in critical sectors such as banking, healthcare, and government services. The architecture integrates **artificial intelligence, continuous identity verification, threat intelligence analytics, and automated security enforcement** to ensure secure access and resilient infrastructure operations.

At the foundation of the framework is the **cloud-native infrastructure layer**, which hosts enterprise workloads including financial systems, healthcare data platforms, and government digital services. This layer typically consists of **containerized applications, microservices, serverless environments, and distributed cloud storage**, enabling scalable and flexible deployment across hybrid and multi-cloud environments.

Above the infrastructure layer is the **identity and access management layer**, which implements the core principle of **Zero Trust security**: never trust, always verify. Every user, device, and application attempting to access the system must undergo continuous authentication and authorization processes. This layer uses identity verification mechanisms, role-based access control, and device posture validation to prevent unauthorized access.

The **AI-driven security intelligence layer** forms the analytical core of the architecture. It uses machine learning models and behavioral analytics to analyze user activities, network traffic, and system logs in real time. By identifying abnormal patterns and suspicious activities, the AI system can detect insider threats, unauthorized access attempts, and potential cyberattacks before they escalate.

A **security orchestration and automated response layer** coordinates responses to detected threats. When anomalies or policy violations are identified, the system automatically triggers mitigation actions such as access restriction, workload isolation, vulnerability patching, or incident alerts. This automated response mechanism reduces reaction time and enhances overall system resilience.

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

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

DOI: 10.15680/IJCTECE.2025.0806029

The framework also includes a **continuous monitoring and compliance management layer**, which ensures that organizational policies and regulatory requirements are consistently enforced. Security logs, audit trails, and compliance reports are generated and monitored to maintain transparency and regulatory adherence, particularly important in sectors handling sensitive financial, healthcare, or government data.

Overall, this architecture demonstrates how **AI-enhanced Zero Trust principles** can provide robust protection for critical digital infrastructures. By combining intelligent threat detection, strict identity verification, automated security enforcement, and continuous monitoring, the framework creates a secure and adaptive cybersecurity environment capable of defending complex cloud-native ecosystems.

The second stage focuses on **data collection and security monitoring**. Security logs, network traffic data, authentication records, and system behavior information are continuously collected from cloud infrastructure and application environments. This data provides the foundation for training AI models and monitoring system activities.

The third stage involves **AI-based threat detection and behavioral analysis**. Machine learning algorithms analyze historical and real-time data to identify abnormal user behavior, suspicious network activities, and potential security breaches. The system builds behavioral profiles for users and devices, allowing it to detect deviations that may indicate malicious activity.

The fourth stage is **Zero Trust implementation and continuous authentication**. Identity verification mechanisms such as multi-factor authentication, device verification, and contextual access control are integrated into the system. Every access request is evaluated based on risk level, user identity, device health, and location. High-risk activities trigger additional verification steps or access restrictions.

The fifth stage focuses on **automated threat response and security orchestration**. When the AI system detects a potential threat, automated response mechanisms are triggered. These responses may include blocking suspicious connections, isolating compromised systems, revoking access privileges, or alerting security administrators. Automation reduces response time and prevents potential data breaches.

Finally, the framework is evaluated using **security performance metrics** such as threat detection accuracy, response time, false positive rate, and system scalability. These metrics help determine the effectiveness of the proposed cybersecurity framework in protecting cloud-native systems.

Applications in Critical Sectors

Banking Systems:

In the banking sector, the proposed framework protects digital payment platforms, online banking services, and financial transaction systems. AI-driven monitoring can detect fraudulent activities, unusual transaction patterns, and unauthorized access attempts. Continuous authentication and Zero Trust access policies ensure that only authorized users and systems can access financial data.

Healthcare Systems:

Healthcare organizations manage large volumes of sensitive patient data through electronic health records and telemedicine platforms. The Zero Trust AI framework helps secure medical data by enforcing strict identity verification and monitoring access to healthcare applications. AI-based anomaly detection can identify unauthorized attempts to access patient records or manipulate medical data.

Government Systems:

Government institutions manage critical infrastructure, citizen databases, and confidential national information. The proposed framework provides secure access control for government networks and ensures that only authorized personnel can access sensitive information. AI-driven threat intelligence helps detect cyber espionage, insider threats, and advanced persistent attacks targeting government systems.

Advantages of the Proposed Framework

The integration of AI and Zero Trust security provides several advantages for protecting cloud-native systems. Continuous verification ensures that no user or device is automatically trusted, reducing the risk of unauthorized access. AI-powered analytics improves threat detection by identifying anomalies that traditional security systems may overlook.

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

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

DOI: 10.15680/IJCTECE.2025.0806029

Automation enhances the efficiency of incident response by enabling rapid threat containment and mitigation. The cloud-native architecture also provides scalability and flexibility, allowing organizations to adapt to changing security requirements and growing data volumes. These features make the framework particularly suitable for high-security sectors such as banking, healthcare, and government services.

IV. RESULTS AND DISCUSSION

The proposed **Zero Trust AI-powered cybersecurity framework** was evaluated using simulated cloud-native environments representing banking, healthcare, and government systems. The evaluation focused on measuring the effectiveness of AI-based threat detection, access control efficiency, vulnerability identification, and automated response performance. Security logs, network traffic data, authentication records, and simulated cyberattack scenarios were used to test the framework.

The results indicate that integrating **artificial intelligence with Zero Trust security principles** significantly improves the overall security posture of cloud-native systems. The AI-based threat detection model successfully identified abnormal user behavior, unauthorized access attempts, and suspicious network activities with high accuracy. Machine learning algorithms analyzed large volumes of security data and detected patterns associated with potential cyber threats much faster than traditional rule-based security systems.

The implementation of **continuous authentication and identity-based access control** also demonstrated strong improvements in preventing unauthorized access. Every user, device, and application was required to undergo verification before accessing system resources. This approach reduced the risk of insider threats and credential misuse. Multi-factor authentication and contextual access evaluation ensured that access privileges were granted only under secure conditions.

The **automated threat response mechanisms** significantly reduced incident response time. When the AI system detected suspicious activity, automated security orchestration tools immediately triggered response actions such as blocking network connections, isolating compromised containers, or restricting user access. This rapid response capability helped minimize the potential impact of cyberattacks and prevented the spread of malicious activities within the network.

The framework also demonstrated strong performance in **protecting sector-specific systems**. In banking environments, the AI model detected unusual transaction patterns and potential fraud attempts. In healthcare systems, the framework successfully monitored access to patient records and prevented unauthorized attempts to retrieve sensitive medical data. In government systems, the architecture effectively detected suspicious access patterns and potential insider threats targeting confidential information.

Despite these positive results, several challenges were observed during implementation. AI models require high-quality datasets to maintain accurate predictions. Incomplete or inconsistent security data can reduce the effectiveness of threat detection models. Additionally, integrating AI systems with existing enterprise infrastructure may require significant computational resources and careful configuration.

Overall, the experimental results demonstrate that the proposed framework provides **improved threat detection, faster response times, and stronger access control** compared to traditional security approaches. By combining Zero Trust principles with AI-driven cybersecurity analytics, organizations can significantly enhance the security of cloud-native systems used in critical sectors such as banking, healthcare, and government services.

V. CONCLUSION

The increasing adoption of **cloud-native architectures** in critical sectors such as banking, healthcare, and government has brought both opportunities and cybersecurity challenges. Traditional perimeter-based security models are no longer sufficient for protecting highly distributed and dynamic infrastructures. This paper proposed a **Zero Trust AI-powered cybersecurity framework** that integrates continuous authentication, identity-centric access control, AI-driven threat detection, and automated response mechanisms to secure cloud-native systems.

The framework ensures that every user, device, and application is continuously verified before accessing sensitive resources, significantly reducing the risk of unauthorized access and insider threats. AI algorithms analyze large volumes of security data to detect anomalies, identify potential vulnerabilities, and provide predictive threat intelligence. Automated orchestration allows for rapid mitigation of detected threats, minimizing operational disruption. Experimental evaluation in simulated

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

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

DOI: 10.15680/IJCTECE.2025.0806029

environments demonstrated improved threat detection accuracy, faster incident response, and enhanced resilience for autonomous enterprise systems.

By combining **Zero Trust principles with AI-driven cybersecurity**, the proposed framework provides a robust, proactive, and adaptive security solution suitable for cloud-native banking, healthcare, and government infrastructures. It offers a scalable approach to safeguarding critical digital assets while maintaining operational efficiency and compliance with industry regulations.

VI. FUTURE WORK

Future research on the **Zero Trust AI-powered cybersecurity framework** can focus on several key areas to enhance its effectiveness, adaptability, and applicability across complex cloud-native environments. One important direction is the development of **advanced AI models**, including deep learning and reinforcement learning techniques, to improve anomaly detection, predictive vulnerability analysis, and real-time threat classification. Such models can better identify sophisticated attack patterns that traditional machine learning algorithms may overlook.

Another promising area is **federated learning**, which enables multiple organizations, such as banks, hospitals, or government agencies, to collaboratively train AI models without sharing sensitive data. This approach enhances threat intelligence while maintaining data privacy and compliance with sector-specific regulations. Additionally, incorporating **explainable AI (XAI)** can improve transparency in threat detection and decision-making processes, allowing security analysts to understand why the system flags certain activities as suspicious, which is critical for trust, accountability, and regulatory compliance.

Future work should also address **multi-cloud and hybrid infrastructure environments**, ensuring that Zero Trust policies and AI-driven security mechanisms are consistently enforced across diverse platforms. Integrating **blockchain-based security mechanisms** can provide immutable audit trails, secure identity management, and enhanced data integrity, which are particularly valuable for critical sectors handling sensitive financial, health, or governmental data.

Finally, research can focus on enhancing **self-healing cyber resilience**, where the system not only detects and mitigates threats automatically but also learns from each incident to strengthen defenses over time. By pursuing these enhancements, the framework can evolve into a more comprehensive, intelligent, and adaptive cybersecurity solution capable of securing cloud-native enterprise systems against emerging threats while maintaining operational continuity and compliance.

REFERENCES

1. Kamadi, S. (2025). Machine learning and AI architecture: A comprehensive framework for production-grade intelligent systems. World Journal of Advanced Research and Reviews, 27(1), 2789–2799.
2. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
3. Grandhe, K. (2025). Designing a Scalable Data Lake Architecture on AWS Using Glue and S3. International Journal of Artificial Intelligence Data Science and Machine Learning, 6(3), 60-63.
4. Gurajapu, A., Anumolu, S., Garimella, V., Chundi, V. M. S. R., & Gubbala, V. S. A. P. (2025). Ethical and Trustworthy Autonomous Agents in Network SecOps: Transparency, Auditing, and Human-in-the-Loop Overrides. Frontiers in Computer Science and Artificial Intelligence, 4(2), 63-66.
5. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology, 15(6), 653-662.
6. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research, 6(4), 8419-8426.
7. Gadige, C. D. (2025). The evolution of user interface development in Salesforce: From Visualforce to Lightning Web Components. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 8(5), 12883–12890.
8. Ambati, K. C. (2024). Enterprise-wide procurement consolidation: Ivalua-SAP-EDW integration architecture for global supply chain excellence. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 7(4), 14309–14318.
9. Parathraju, P., & Umasankar, P. (2025). Performance evaluation of ultrathin CdTe-based solar cells with dual absorbers via SCAPS-1D simulation. Scientific Reports, 15(1), 26428.

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

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

DOI: 10.15680/IJCTECE.2025.0806029

10. Vijayakumar, R., & Gireesh, G. (2013, July). Quantitative analysis and fracture detection of pelvic bone X-ray images. In 2013 Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
11. 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.
12. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
13. Gowda, M. K. S. (2025). Driving Return on Risk-Weighted Assets Improvement via Audit, Analytics, and Advanced Modeling in Bank Portfolio Management. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12197-12206.
14. S. Vishwarup et al. (2020). Automatic Person Count Indication System using IoT in a Hotel Infrastructure. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4).
15. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
16. 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.
17. Surampudi, Y., Kondaveeti, D., & Pichaimani, T. (2023). A Comparative Study of Time Complexity in Big Data Engineering: Evaluating Efficiency of Sorting and Searching Algorithms in Large-Scale Data Systems. Journal of Science & Technology, 4(4), 127-165.
18. Viswanathan, Venkatraman. "AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization." (2023).
19. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
20. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
21. 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.
22. Panda, S. S. (2024). Delivering Scalable Cloud Services in China: Microsoft and 21Vianet Collaboration. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11325-11333.
23. Muthusamy, P., Muthirevula, G. R., & Mohammed, A. S. (2025). Zero-Touch Continuous Audit with Hybrid Symbolic-Neural Reasoning. Newark Journal of Human-Centric AI and Robotics Interaction, 5, 80-111.
24. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-Based Extreme Learning Machines for Mining Waste Detoxification Efficiency. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1348-1353). IEEE.
25. Kalra, S., Faiz, A., Aggarwal, D., Vigenesh, M., Ramesh, P. N., & Elais, S. (2025, December). Optimizing CNNR-NNT Model for Effective Product Recommendation in E-Commerce. In 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU) (pp. 1-7). IEEE.
26. Konda, S. K. (2024). Carbon-native DCIM architectures for AI data centers: Autonomous infrastructure control via smart grid intelligence. World Journal of Advanced Research and Reviews, 21(1), 3008–3318.
27. Thumala, S. R., Madathala, H., & Sharma, S. (2025, March). Towards Sustainable Cloud Computing: Innovations in Energy-Efficient Resource Allocation. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1528-1533). IEEE.
28. Suddala, V. R. A. K. (2025, November). FADL-DP and CNN-GRU Driven Cloud Framework for Secure Healthcare E-Commerce Platform. In 2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 991-996). IEEE.
29. Jothilingam, P. (2025). Towards autonomous commissioning: Integrating digital twins artificial intelligence and smart sensors for next-generation process control systems. Certified Journal of International Research, 5(1), 1-8.
30. Ramidi, M. (2024). Securing Mobile App Development with Compliance Aware CI/CD Pipelines in Government. International Journal of Computer Technology and Electronics Communication, 7(3), 8824-8825.
31. Karnam, A. (2023). SAP Beyond Uptime: Engineering Intelligent AMS with High Availability & DR through Pacemaker Automation. International Journal of Research Publications in Engineering, Technology and Management, 6(5), 9351□9361. https://doi.org/10.15662/IJRPETM.2023.0605011
32. 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.

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

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

DOI: 10.15680/IJCTECE.2025.0806029

33. Pothuri, M. K. (2025). The role of data governance in achieving compliance and trust in healthcare and fintech. IJAIDR□Journal of Advances in Developmental Research, 16(2).
34. Shewale, V. (2025). The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age. European Journal of Computer Science and Information Technology, 13(15), 11-20.
35. Sarabu, V. B. (2022). Hybrid on-premise to cloud data migration: A controlled one-way synchronization framework for enterprise-scale modernization. International Journal of Science, Research and Technology, 5(5), 19-33.
36. 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.
37. Anumula, S. R. (2025). Real-Time Scheduling Optimization Using Machine Learning in Pilot Trading and Tracking Systems. Journal Of Multidisciplinary, 5(7), 128-133.
38. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
39. Uttama Reddy Sanepalli. (2022). 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, 8(6), 769-780.
40. Gaddapuri, N. S. (2025). Digital twin governance: IoT-driven real-time regulatory auditing in smart hospital architecture. International Journal of Computer Technology and Electronics Communication, 8(5), 11515–11524.