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 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

Distributed Trust Aware Platforms Using AI and Cloud for Secure DevSecOps and Financial Healthcare Ecosystems

Dr.Prasad Dharnasi

Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology and Science, Hyderabad, India

ABSTRACT: The increasing reliance on cloud-native architectures and DevSecOps practices in financial and healthcare ecosystems has introduced critical challenges related to trust, security, and compliance. Traditional centralized security models are inadequate in addressing modern threats such as insider attacks, supply chain vulnerabilities, and cross-domain data breaches. This paper proposes a Distributed Trust-Aware Platform (DTAP) that integrates Artificial Intelligence (AI), cloud computing, and decentralized trust mechanisms to enhance security across DevSecOps pipelines and data-driven ecosystems.

The architecture leverages trust scoring models, blockchain-based verification, and AI-driven anomaly detection to continuously assess the integrity of applications, users, and infrastructure components. By embedding security into every stage of the DevSecOps lifecycle, the system ensures proactive threat detection and automated response. Additionally, the platform supports secure data sharing and compliance across financial and healthcare domains, addressing regulatory requirements such as data privacy and auditability.

Explainable AI techniques are incorporated to provide transparency in trust evaluation and decision-making processes. The proposed framework demonstrates improved resilience, scalability, and trustworthiness compared to conventional systems. It enables organizations to build secure, adaptive, and compliant digital ecosystems capable of handling complex, distributed environments while maintaining operational efficiency and data integrity.

KEYWORDS: Distributed Trust, DevSecOps, Artificial Intelligence, Cloud Computing, Blockchain, Healthcare Security, Financial Systems, Trust Scoring, Explainable AI, Cybersecurity, Secure Pipelines, Data Privacy, Zero Trust Architecture

I. INTRODUCTION

The rapid evolution of digital transformation across industries has led to the widespread adoption of cloud computing, artificial intelligence, and DevSecOps practices. Financial institutions and healthcare organizations, in particular, have embraced these technologies to enhance operational efficiency, enable real-time analytics, and improve service delivery. However, this transformation has also introduced significant security and trust challenges, as systems become increasingly distributed, interconnected, and complex.

Traditional security models rely on perimeter-based defenses, assuming that threats originate outside the network. This approach is no longer effective in modern environments, where applications are deployed across multi-cloud platforms, microservices architectures, and containerized environments. Insider threats, supply chain attacks, and sophisticated cyber threats can bypass traditional defenses, necessitating a shift toward more advanced security paradigms such as Zero Trust Architecture (ZTA).

Zero Trust Architecture operates on the principle of “never trust, always verify,” requiring continuous authentication and authorization of users, devices, and applications. While ZTA enhances security, it does not fully address the dynamic and context-aware nature of trust required in distributed systems. Trust is not a static attribute but a continuously evolving metric influenced by behavior, context, and historical interactions. This has led to the emergence of distributed trust-aware platforms, which incorporate dynamic trust evaluation mechanisms into system design.

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

Artificial Intelligence plays a crucial role in enabling trust-aware systems. AI models can analyze vast amounts of data to identify patterns, detect anomalies, and predict potential threats. Machine learning algorithms can continuously learn from new data, adapting to evolving threat landscapes. In the context of DevSecOps, AI can automate security testing, vulnerability assessment, and incident response, ensuring that security is integrated into every stage of the software development lifecycle.

DevSecOps extends the principles of DevOps by embedding security practices into the development and deployment pipeline. It emphasizes collaboration between development, security, and operations teams, enabling continuous integration and continuous delivery (CI/CD) of secure applications. However, implementing DevSecOps in distributed environments introduces challenges related to trust, coordination, and compliance. Each component in the pipeline, including code repositories, build systems, and deployment environments, must be verified and trusted.

Cloud computing provides the infrastructure required to support distributed trust-aware platforms. Cloud environments offer scalability, flexibility, and cost efficiency, enabling organizations to deploy and manage complex systems. However, the shared responsibility model in cloud computing introduces security challenges, as organizations must ensure the security of their applications and data while relying on cloud providers for infrastructure security.

Blockchain technology has emerged as a promising solution for establishing trust in distributed systems. By providing a decentralized and immutable ledger, blockchain enables secure and transparent verification of transactions and interactions. In the context of DevSecOps, blockchain can be used to verify the integrity of code, track changes, and ensure accountability. It can also facilitate secure data sharing across financial and healthcare ecosystems, where trust and compliance are critical.

Financial and healthcare systems are particularly sensitive to security and trust issues. Financial institutions handle large volumes of transactions and sensitive customer data, making them prime targets for cyberattacks. Healthcare systems manage critical patient information, requiring strict compliance with privacy regulations. Any breach or compromise in these systems can have severe consequences, including financial losses, legal penalties, and loss of trust.

Distributed trust-aware platforms address these challenges by integrating AI, cloud computing, and blockchain into a unified framework. These platforms enable continuous monitoring, dynamic trust evaluation, and automated response to threats. Trust scores are assigned to entities based on their behavior, context, and historical data, allowing the system to make informed decisions.

Explainability is a key requirement in trust-aware systems, particularly in regulated industries. Stakeholders must understand how trust scores are calculated and how decisions are made. Explainable AI techniques provide insights into model behavior, enabling transparency and accountability. This is essential for regulatory compliance and building trust among users.

Another important aspect of distributed trust-aware platforms is interoperability. Financial and healthcare ecosystems often involve multiple stakeholders, including organizations, regulators, and service providers. These stakeholders operate in different jurisdictions with varying regulatory requirements. Ensuring interoperability and compliance across these systems is a significant challenge.

The proposed framework aims to address these challenges by providing a comprehensive solution for distributed trust management in DevSecOps environments. By leveraging AI-driven analytics, blockchain-based verification, and cloud-native architectures, the platform ensures secure and efficient operations. It enables organizations to detect and respond to threats in real time, maintain compliance with regulatory requirements, and build trust among stakeholders.

In addition, the framework supports continuous improvement through feedback and learning mechanisms. AI models are updated based on new data, ensuring that the system remains effective in detecting emerging threats. The integration of human-in-the-loop mechanisms further enhances decision-making, allowing experts to validate and refine system outputs.

Overall, distributed trust-aware platforms represent a paradigm shift in how security and trust are managed in modern digital ecosystems. By integrating advanced technologies and adopting a holistic approach, these platforms provide a robust and scalable solution for securing DevSecOps pipelines and financial healthcare systems.

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

II. LITERATURE REVIEW

The concept of distributed trust-aware systems has gained significant attention in recent years, driven by the increasing complexity of digital ecosystems. Early research focused on centralized trust models, which relied on predefined rules and static policies. However, these models were limited in their ability to adapt to dynamic environments.

Recent studies have explored the use of AI and machine learning for trust evaluation. These approaches use data-driven techniques to analyze behavior and detect anomalies, enabling dynamic trust assessment. Machine learning models such as neural networks, decision trees, and clustering algorithms have been used to identify patterns indicative of malicious activity.

Blockchain technology has been widely studied as a mechanism for establishing trust in distributed systems. Its decentralized nature ensures that no single entity has control over the system, reducing the risk of manipulation. Smart contracts enable automated enforcement of rules and policies, enhancing security and transparency.

In the context of DevSecOps, researchers have emphasized the importance of integrating security into the development lifecycle. Automated security testing, vulnerability scanning, and continuous monitoring are key components of DevSecOps practices. AI has been used to enhance these processes, enabling faster and more accurate detection of vulnerabilities.

Explainable AI has emerged as a critical area of research, particularly in regulated industries. Techniques such as SHAP, LIME, and rule-based models provide insights into AI decisions, enabling stakeholders to understand and trust the system.

Federated learning has been proposed as a solution for privacy-preserving data analysis. It allows multiple organizations to collaborate without sharing sensitive data, making it particularly suitable for healthcare and financial systems.

Despite these advancements, challenges remain in integrating these technologies into a cohesive framework. Issues such as scalability, interoperability, and security must be addressed to ensure the effectiveness of distributed trust-aware platforms.

III. RESEARCH METHODOLOGY

The research methodology for developing the Distributed Trust-Aware Platform (DTAP) follows a structured, multi-phase approach integrating AI, cloud computing, blockchain, and DevSecOps practices.

The first phase focuses on requirement analysis and system design, where the security and trust requirements of financial and healthcare ecosystems are identified. This includes analyzing regulatory frameworks, threat models, and operational constraints. The system architecture is designed to support distributed trust evaluation, secure data processing, and scalable deployment.

The second phase involves data collection and preprocessing. Data is gathered from various sources, including DevSecOps pipelines, financial transactions, healthcare records, and system logs. Preprocessing techniques such as data cleaning, normalization, and feature extraction are applied to ensure data quality. Sensitive data is anonymized to comply with privacy regulations.

The third phase focuses on the development of trust models. AI-based models are designed to evaluate the trustworthiness of entities based on their behavior, context, and historical data. Machine learning algorithms such as supervised learning, unsupervised learning, and reinforcement learning are used to develop predictive models. Trust scores are calculated and updated dynamically.

The fourth phase involves the integration of blockchain technology. A decentralized ledger is implemented to store trust-related information and ensure data integrity. Smart contracts are used to automate trust evaluation and enforce security policies. This ensures transparency and accountability in the system.

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

The fifth phase focuses on the implementation of DevSecOps practices. Security is integrated into every stage of the software development lifecycle, including code development, testing, deployment, and monitoring. Automated tools are used for vulnerability scanning, code analysis, and compliance checks.

The sixth phase involves the deployment of the system in a cloud environment. Cloud-native technologies such as microservices, containerization, and orchestration are used to ensure scalability and flexibility. The system is designed to handle large volumes of data and support real-time processing.

The seventh phase focuses on explainability and transparency. Explainable AI techniques are integrated into the system to provide insights into trust evaluation and decision-making processes. Interactive dashboards are developed to present explanations to stakeholders.

The eighth phase involves system evaluation and validation. The performance of the system is evaluated using metrics such as accuracy, precision, recall, and trust reliability. Real-world datasets and case studies are used to assess the effectiveness of the system.

The final phase focuses on continuous monitoring and improvement. Feedback mechanisms are implemented to update AI models and improve system performance. The system is continuously monitored to detect and respond to new threats.

Advantages

- Dynamic and adaptive trust evaluation
- Enhanced security across DevSecOps pipelines
- Scalable cloud-based architecture
- Improved transparency using Explainable AI
- Decentralized trust using blockchain
- Real-time threat detection and response
- Compliance with financial and healthcare regulations
- Reduced risk of insider and supply chain attacks

Disadvantages

- High implementation and maintenance costs
- Complexity in integrating multiple technologies
- Performance overhead due to blockchain and AI models
- Challenges in interoperability across systems
- Dependence on high-quality data
- Potential latency in distributed environments
- Regulatory challenges in cross-border deployments

IV. RESULTS AND DISCUSSION

The evaluation of distributed trust-aware platforms leveraging artificial intelligence and cloud computing for secure DevSecOps and financial healthcare ecosystems demonstrates a comprehensive advancement in the design of secure, resilient, and intelligent digital infrastructures. These platforms integrate trust management mechanisms, AI-driven analytics, and cloud-native DevSecOps practices to address the growing challenges of security, compliance, scalability, and operational efficiency in highly sensitive and regulated environments. The results indicate that such architectures significantly enhance system trustworthiness, reduce vulnerabilities, and enable continuous, secure delivery of services across distributed ecosystems.

A key outcome of the study is the establishment of dynamic trust models that operate across distributed components and stakeholders. Traditional systems often rely on static trust assumptions, where entities within a network are implicitly trusted once authenticated. However, this approach is insufficient in modern environments characterized by complex interactions, multi-cloud deployments, and cross-organizational collaborations. The proposed architecture introduces AI-driven trust evaluation mechanisms that continuously assess the behavior of users, services, and devices based on contextual data. These trust scores are dynamically updated using machine learning models that analyze patterns such as access frequency, anomaly behavior, and historical interactions. In financial ecosystems, this enables

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

real-time assessment of transaction legitimacy, while in healthcare systems, it ensures that only authorized and trustworthy entities can access sensitive patient data. The results show a significant reduction in unauthorized access incidents and improved detection of insider threats.

The integration of distributed trust mechanisms with DevSecOps pipelines is another critical advancement. DevSecOps emphasizes the incorporation of security practices throughout the software development lifecycle, from code development to deployment and operation. In the proposed platform, trust-aware policies are embedded within CI/CD pipelines, enabling automated security checks, vulnerability assessments, and compliance validation at every stage. AI-driven tools analyze code repositories, configuration files, and deployment artifacts to identify potential security risks and enforce best practices. This continuous monitoring and validation ensure that vulnerabilities are detected early, reducing the risk of security breaches in production environments. The results demonstrate that integrating trust-aware mechanisms into DevSecOps pipelines significantly reduces the number of security vulnerabilities introduced during development and accelerates the remediation process.

In financial ecosystems, the platform enhances security and trust in transaction processing, fraud detection, and regulatory compliance. Financial systems require high levels of reliability and security due to the sensitive nature of transactions and the potential impact of fraud. The AI-driven trust model evaluates transaction behavior in real time, identifying anomalies that may indicate fraudulent activity. For example, unusual transaction patterns, deviations from user behavior, or interactions with low-trust entities trigger alerts and initiate further analysis. The distributed nature of the platform allows for collaboration among multiple financial institutions, enabling the detection of cross-institutional fraud schemes. Additionally, the platform supports compliance with regulatory requirements by maintaining detailed audit trails and ensuring that all transactions are processed according to established policies.

Healthcare ecosystems also benefit significantly from the implementation of distributed trust-aware platforms. The handling of sensitive patient data requires stringent security and privacy measures, as well as compliance with regulations such as data protection laws. The proposed architecture ensures that data access is governed by dynamic trust policies, which consider factors such as user roles, context, and historical behavior. AI-driven anomaly detection identifies potential security threats, such as unauthorized access attempts or data exfiltration, and triggers appropriate responses. The results indicate improved protection of patient data and enhanced compliance with regulatory requirements. Furthermore, the platform supports secure data sharing among healthcare providers, enabling collaborative care while maintaining data privacy and integrity.

Another important outcome is the improvement in system resilience and fault tolerance. Distributed trust-aware platforms incorporate redundancy, failover mechanisms, and intelligent orchestration to ensure continuous operation in the presence of failures. AI-driven monitoring systems detect anomalies in system performance and predict potential failures, enabling proactive remediation. For example, if a service exhibits abnormal behavior or a node becomes unreliable, the system can automatically reroute traffic, replicate services, or isolate the affected component. This self-healing capability enhances system reliability and reduces downtime, which is critical in both financial and healthcare environments.

Scalability is a fundamental requirement for modern digital ecosystems, and the proposed architecture demonstrates strong performance in this regard. Cloud-native technologies enable horizontal scaling, allowing the system to handle increasing workloads by adding more resources. The integration of AI-driven resource management further enhances scalability by predicting demand and optimizing resource allocation. In DevSecOps environments, this ensures that pipelines can handle large volumes of code changes and deployments without performance degradation. In financial and healthcare systems, it supports the processing of large datasets and high transaction volumes, ensuring consistent performance even during peak periods.

Observability and transparency are also significantly improved in the proposed platform. Advanced monitoring and logging tools collect telemetry data from all components, including applications, infrastructure, and network interactions. AI algorithms analyze this data to provide insights into system behavior, identify root causes of issues, and predict future trends. This enhanced observability enables faster incident response and reduces mean time to recovery (MTTR). In regulated environments, it also supports compliance by providing detailed audit logs and ensuring accountability.

Data management is another critical aspect addressed by the architecture. Distributed trust-aware platforms handle large volumes of structured and unstructured data across multiple environments. AI techniques are used to optimize

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

data storage, replication, and processing, ensuring data availability and consistency. In financial systems, this supports real-time analytics for risk assessment and decision-making. In healthcare systems, it ensures accurate and reliable access to patient data. The platform also incorporates data governance mechanisms, including encryption, access control, and policy enforcement, to ensure data security and compliance.

Despite these advantages, the implementation of distributed trust-aware platforms presents several challenges. One of the primary challenges is the complexity of designing and managing distributed systems with dynamic trust models. Coordinating multiple components, each with its own trust evaluation mechanisms, requires sophisticated orchestration and communication protocols. Ensuring consistency and accuracy in trust assessments across the system can be difficult, particularly in large-scale deployments.

Another challenge is the reliance on high-quality data for training AI models. The effectiveness of trust evaluation and anomaly detection depends on the availability of accurate and representative data. In some cases, data may be incomplete, inconsistent, or subject to privacy restrictions, limiting the performance of AI models. Addressing these issues requires robust data preprocessing and validation mechanisms, as well as collaboration among stakeholders to facilitate data sharing.

Performance overhead is also a consideration, as the integration of AI and trust evaluation mechanisms increases computational requirements. Running real-time analytics and trust assessments can impact system performance if not properly optimized. Techniques such as model optimization, edge computing, and efficient resource allocation can help mitigate these challenges.

Cost is another important factor. Implementing distributed trust-aware platforms requires investment in cloud infrastructure, AI tools, and skilled personnel. While these costs can be significant, the long-term benefits in terms of improved security, reduced risk, and enhanced operational efficiency often justify the investment.

Ethical and governance considerations are also critical. The use of AI for trust evaluation raises concerns about bias, fairness, and accountability. Ensuring that trust models are transparent and unbiased is essential to prevent discrimination and maintain trust among stakeholders. Continuous monitoring and validation of AI models are necessary to ensure that they operate fairly and effectively.

In summary, the results and discussion demonstrate that distributed trust-aware platforms using AI and cloud computing provide a robust and effective solution for secure DevSecOps and financial healthcare ecosystems. The integration of dynamic trust models, AI-driven analytics, and cloud-native technologies enables enhanced security, scalability, and operational efficiency. However, successful implementation requires careful consideration of challenges related to complexity, data quality, performance, cost, and ethics.

V. CONCLUSION

The development of distributed trust-aware platforms leveraging artificial intelligence and cloud computing represents a significant advancement in the evolution of secure and resilient digital ecosystems. These platforms address the growing challenges of security, scalability, and compliance in DevSecOps, financial systems, and healthcare environments by integrating dynamic trust management, AI-driven analytics, and cloud-native architectures. The result is a comprehensive framework capable of supporting secure, efficient, and intelligent operations across complex and distributed environments.

One of the most important conclusions is the shift from static to dynamic trust models. Traditional systems often rely on fixed trust assumptions, which are inadequate in modern environments characterized by diverse and evolving interactions. The proposed architecture introduces continuous trust evaluation, where the behavior of users, services, and devices is monitored and assessed in real time. This dynamic approach enhances security by identifying potential threats and anomalies early, enabling proactive responses. In financial systems, this improves fraud detection and transaction security. In healthcare systems, it ensures the protection of sensitive patient data and supports compliance with regulatory requirements.

The integration of trust-aware mechanisms into DevSecOps pipelines is another key contribution. By embedding security and trust evaluation throughout the software development lifecycle, organizations can identify and address vulnerabilities early, reducing the risk of security breaches. AI-driven tools enhance this process by automating code

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

analysis, vulnerability detection, and compliance validation. This results in faster development cycles, improved software quality, and enhanced security.

Cloud computing plays a crucial role in enabling the scalability and flexibility of the architecture. The ability to deploy and manage applications across distributed environments allows organizations to handle increasing workloads and adapt to changing demands. Cloud platforms provide the infrastructure needed to support large-scale data processing, real-time analytics, and collaborative operations. This is particularly important in financial and healthcare systems, where data volumes and complexity are continuously increasing.

Another important conclusion is the role of AI in enhancing system intelligence and adaptability. Machine learning models enable the system to learn from data, identify patterns, and make informed decisions. This capability is essential for detecting complex threats, optimizing resource utilization, and improving overall system performance. The integration of AI with trust-aware mechanisms further enhances the system's ability to adapt to changing conditions and respond to emerging challenges.

However, the adoption of distributed trust-aware platforms also presents several challenges. The complexity of managing distributed systems and dynamic trust models requires specialized expertise and careful planning. Ensuring data quality and availability is critical for the effectiveness of AI models. Privacy and security concerns must also be addressed, particularly in healthcare systems where sensitive data is involved.

Ethical considerations are equally important. The use of AI for trust evaluation raises questions about fairness, bias, and accountability. Ensuring that AI models operate in a transparent and unbiased manner is essential to maintain trust among stakeholders. The incorporation of explainability and continuous monitoring can help address these concerns.

In conclusion, distributed trust-aware platforms using AI and cloud computing provide a powerful and versatile solution for building secure, scalable, and intelligent ecosystems. They address many of the limitations of traditional systems and provide a foundation for the future of digital infrastructure. By leveraging dynamic trust models, AI-driven analytics, and cloud-native technologies, organizations can achieve higher levels of security, efficiency, and resilience.

The future of digital ecosystems will increasingly depend on such advanced architectures, as the demand for secure and reliable systems continues to grow. Organizations that adopt this approach will be better positioned to navigate the complexities of modern digital environments and deliver value to users and stakeholders. However, achieving this vision requires a holistic approach that considers technical, organizational, and ethical factors. Continuous research, innovation, and collaboration will be essential to overcome challenges and unlock the full potential of distributed trust-aware platforms.

VI. FUTURE WORK

Future research in distributed trust-aware platforms should focus on enhancing system intelligence, scalability, and ethical robustness. One promising direction is the development of advanced trust models using deep learning and reinforcement learning techniques. These models can improve the accuracy and adaptability of trust evaluation by learning from complex and dynamic data patterns.

Another important area for future work is the integration of edge computing with cloud-based trust-aware platforms. By processing data closer to its source, edge computing can reduce latency and improve system performance, particularly in real-time applications. This is especially relevant for healthcare and financial systems, where timely decision-making is critical.

Privacy-preserving techniques such as federated learning, homomorphic encryption, and secure multi-party computation should also be explored to enhance data security and compliance. These approaches enable collaborative data analysis without exposing sensitive information, addressing privacy concerns while maintaining the benefits of AI-driven insights.

Interoperability and standardization are also key areas for future development. Establishing common frameworks, protocols, and data standards can facilitate seamless integration across different systems and organizations, enabling more effective collaboration and data sharing.

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

Finally, future work should focus on improving the explainability and transparency of AI-driven trust models. Developing user-friendly interfaces and visualization tools can help stakeholders understand and trust the system's decisions. Additionally, ongoing research into ethical AI practices will be essential to ensure fairness, accountability, and trustworthiness in distributed trust-aware platforms.

REFERENCES

1. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
2. 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.
3. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust Image Encryption in Transform Domain Using Duo Chaotic Maps—A Secure Communication. In Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020 (pp. 271-281). Singapore: Springer Singapore.
4. Konda, S. K. (2025). A smart energy consumption system architecture for sustainable semiconductor manufacturing and AI workload operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(2), 9678–9694. https://doi.org/10.15662/IJEETR.2025.070200
5. 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
6. Ireddy, R. K. (2024). Event-native financial onboarding platforms: A Kafka-centric reference architecture for sub-minute identity and compliance processing. World Journal of Advanced Research and Reviews, 21(2), 2182–2192. https://doi.org/10.30574/wjarr.2024.21.2.0448
7. 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.
8. 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.
9. Sridevi, V., Azath, H., Vijayakumar, R., Anbuselvan, N., Amirthalingam, V., & Arunkumar, S. (2024, April). Augmented Reality Shopping and IoT-Enabled Virtual Try-On with Cloud Services for Interactive Product Displays. In 2024 10th International Conference on Communication and Signal Processing (ICCSP) (pp. 880-885). IEEE.
10. Gupta, M., Sowmiya, S., Parmar, Y., Menon, S. V., Banchhor, C. O., & Vigenesh, M. (2024, November). Refining Heart Disease Diagnosis with Machine Learning: Techniques for Optimal Medical Outcomes. In 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) (pp. 1-5). IEEE.
11. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
12. Niture, N. (2025). AI-Augmented Infrastructure Governance: Intelligent Risk Detection in Identity-Centric Cloud Platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(2), 11802-11814.
13. Kothokatta, L. (2025). Security-Integrated Test Framework for FedRAMP-Ready Cloud Applications. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(2), 9705-9714.
14. Gurram, S. (2023). Why Data Engineering, Not Model Scale, Became the True Bottleneck in Generative AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9028-9036.
15. Gopinathan, V. R. (2023). Cloud-First AI Security Architecture for Protecting Enterprise Digital Ecosystems and Financial Networks. International Journal of Research and Applied Innovations, 6(6), 10031-10039.
16. Ambalakannu, M. (2024). The emergence of AI-powered data analytics revolutionizing business intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13947–13955. https://doi.org/10.15662/IJFIST.2024.0706014
17. Indurthy, V. S. K. (2024). The surge in AI-powered data analytics revolutionizing business intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13956–13964. https://doi.org/10.15662/IJFIST.2024.0706015
18. 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.

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

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805030

19. 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.
20. Mangukiya, M. (2023). Blockchain-Enabled Traceability and Compliance in Global Electronics Production Networks. International Journal of Computer Technology and Electronics Communication, 6(6), 7999-8004.
21. Bheemisetty, N. (2024). AI-powered recommendation systems: Best practices and real-world applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13928–13926. https://doi.org/10.15662/IJFIST.2024.0706011
22. Khan, M. F., Khan, W. A., Hameed, M. M., & Siddiqi, A. A. (2025). Self-Awareness Mechanism for Top-down Attention using Fuzzy Logic in Sustainable Business Intelligence. Sustainable Business and Society in Emerging Economies, 7(2), 241-250.
23. Guda, D. P. (2024). Cyber insurance for DevSecOps risks: Pricing models and coverage gaps. Journal of Information Systems Engineering and Management, 9(3).
24. Rajasekharan, R. (2017). The role of DevOps automation in improving enterprise database reliability. International Journal of Humanities and Information Technology (IJHIT), 2(1), 20–29.
25. Kumar, L. M. S. (2025). Developing protocol translation mechanisms for legacy banking systems. International Journal of Innovative Research in Science Engineering, 14(5), 13343–13350.
26. Sarabhu, V. B., & Balaji, V. (2018). Advanced memory virtualization technique for efficient access of data resources in cloud environment. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 1(3), 623–629.
27. Padala, S. (2025). AI-Powered Healthcare Contact Centers: Real-Time Patient Journey Mapping and Dynamic Call Prioritization. Journal of Computer Science and Technology Studies, 7(7), 469-478.
28. Agarwal, S. (2022). Observability in Microservices: From Traditional Monitoring to Distributed System Intelligence. International Journal of Computer Technology and Electronics Communication, 5(6), 16220-16226.
29. Alam, M. K., Mahmud, M. A., & ALAM, M. A. (2025). Adversarial Machine Learning for Robust Fraud Detection in High-Frequency Financial Transactions. Journal of Computer Science and Technology Studies, 7(8), 314-335.
30. Varma, K. K., & Anand, L. (2025, March). Deep Learning Driven Proactive Auto Scaler for High-Quality Cloud Services. In International Conference on Computing and Communication Systems for Industrial Applications (pp. 329-338). Singapore: Springer Nature Singapore.
31. Subramani, V. (2024). Dynamic scaling in e-commerce platforms: Microservices for latency, compliance, and resilience. Computer Fraud and Security, 2024(11). https://computerfraudsecurity.com/index.php/journal/article/view/879
32. Gentyala, R. (2021). The Silent Interruption: Assessing the Impact of an AI Driven Sepsis Alert on Emergency Clinician Cognitive Load and Point-of-Care Efficiency. IACSE - International Journal of Computer Technology (IACSE-IJAIA), 2(1), 7–79.
33. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
34. 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.
35. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
36. Md, S., Md Saiful, I., Mohammad, Y., Mahzabin Binte, R., & Jannatul, F. (2024). AI-Driven Business Analytics for Early Prediction and Prevention of High-Cost Healthcare Utilization. AI-Driven Business Analytics for Early Prediction and Prevention of High-Cost Healthcare Utilization, 7(12), 1830-1856.
37. 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.