International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

Hybrid Federated Learning and Blockchain Ecosystems for Secure Edge Intelligence

Dr. Musheer Vaqur

Department of Computer Application, Tula's Institute Dehradun, U.K., India

musheer77@gmail.com

ABSTRACT: The rapid proliferation of edge devices and distributed IoT infrastructures has heightened the demand for secure, privacy-preserving, and scalable intelligence at the network edge. Federated Learning (FL) has emerged as a transformative approach that enables collaborative model training without centralized data aggregation; however, traditional FL suffers from vulnerabilities such as poisoning attacks, unreliable device participation, single-point aggregation risks, and limited transparency. To address these gaps, this paper proposes a novel **Hybrid Federated Learning and Blockchain Ecosystem** designed to enhance the security, trustworthiness, and resilience of edge intelligence systems. The framework integrates blockchain-based decentralized consensus with FL model updates, ensuring immutability, auditability, and tamper-proof coordination among heterogeneous edge nodes. Smart contracts are used to automate model aggregation, reward honest contributions, and verify update integrity, while a hybrid training architecture combines hierarchical FL, peer-to-peer coordination, and local differential privacy to optimize efficiency and reduce communication overhead. Experimental evaluation across large-scale edge network simulations demonstrates that the proposed hybrid ecosystem significantly improves security against poisoning attacks, increases model accuracy under adversarial conditions, reduces aggregation latency, and achieves higher robustness compared to conventional FL approaches. The results highlight the potential of blockchain-enhanced federated learning as a key enabler of secure, accountable, and high-performance edge intelligence for next-generation IoT environments.

KEYWORDS: Federated Learning; Blockchain; Edge Intelligence; Secure Distributed Learning; Smart Contracts; Decentralized Training; IoT Security; Privacy-Preserving AI; Consensus Mechanisms; Hybrid FL Architecture.

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT), mobile devices, and cyber-physical systems has led to an unprecedented surge in distributed data generation at the network edge. Applications such as smart healthcare, intelligent transportation, industrial automation, and smart grids require real-time intelligence, strict privacy preservation, and continuous system reliability. Traditional cloud-centric machine learning approaches struggle to meet these requirements due to high latency, limited bandwidth, and increasing privacy constraints driven by regulatory frameworks such as GDPR and HIPAA. As a result, **Edge Intelligence**—the paradigm of performing AI computation directly on distributed edge nodes—has emerged as a promising direction for building fast, secure, and context-aware intelligent systems.

Federated Learning (FL) has become one of the cornerstone technologies enabling edge intelligence. FL allows multiple distributed devices to collaboratively train a machine learning model without sharing raw data, thereby significantly enhancing privacy and reducing communication overhead. While FL offers clear advantages, it also faces several critical challenges. First, FL remains vulnerable to data poisoning, model manipulation, and inference attacks, as malicious participants can inject corrupted updates or infer sensitive information from shared gradients. Second, FL typically relies on a centralized aggregator, introducing a single point of failure and limiting transparency in update verification. Third, device heterogeneity, unreliable connectivity, and varying participation rates further degrade model accuracy and system stability.

To address these limitations, researchers have begun exploring the integration of **blockchain technology** with federated learning. Blockchain's decentralized ledger, immutability, and consensus mechanisms provide transparent auditability and tamper-resistant coordination among distributed agents. Smart contracts can automate model aggregation, enforce contribution validation, and ensure accountability across all participants. However, pure blockchain-based FL solutions introduce new challenges, including high computational overhead, increased latency due to consensus protocols, and scalability bottlenecks when deployed in large IoT environments.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

II. LITERATURE REVIEW

The fusion of federated learning (FL) and blockchain has attracted significant attention across academia and industry as edge intelligence grows in scale and complexity. This section reviews the foundational work in Federated Learning, Blockchain for Distributed Systems, their integration for secure decentralized learning, and the remaining challenges that motivate a hybrid ecosystem.

A. Federated Learning in Distributed Edge Environments

Federated Learning, introduced by Google in 2016, has become a leading framework for decentralized model training across diverse edge devices. FL enables collaborative learning by transmitting model updates rather than raw data, thereby preserving privacy and reducing communication costs. FL has been applied in various domains such as mobile keyboard prediction, smart healthcare, autonomous driving, and industrial IoT systems.
However, classical FL suffers from several persistent challenges:

- **Security vulnerabilities:** FL is susceptible to model poisoning, backdoor attacks, and inference attacks.
- **Centralized aggregation risks:** Most FL frameworks depend on a single central server, creating a bottleneck and potential failure point.
- **Device heterogeneity:** Edge nodes differ in computing power, data quality, and availability, causing imbalanced contributions.
- **Limited transparency:** Model aggregation lacks verifiable auditing mechanisms, making it difficult to detect malicious updates.

Recent advancements have proposed enhancements such as hierarchical FL, secure aggregation protocols, differential privacy, and asynchronous FL. While these approaches address certain weaknesses, they still rely on trust in centralized or semi-centralized coordinators and cannot guarantee immutability or accountability across distributed participants.

B. Blockchain for Decentralized Trust and Security

Blockchain introduces decentralization, transparency, and tamper-resistant data management—attributes highly relevant to secure distributed learning. Its consensus protocols (PoW, PoS, PBFT, DPoS) ensure that participating nodes maintain a consistent global ledger without relying on centralized authorities. Smart contracts automate transactions, enforce rules, and maintain verifiable audit trails.
Applications in supply chain management, healthcare, identity verification, and distributed IoT networks show blockchain's effectiveness in establishing trust among untrusted entities.
However, blockchain also faces obstacles:

- **High computational overhead:** Proof-of-Work and other consensus algorithms can be resource-intensive.
- **Latency issues:** Consensus and block propagation introduce delays unsuitable for time-critical edge applications.
- **Scalability limitations:** As blockchain networks grow, throughput may degrade due to block size and propagation constraints.
- **Storage overhead:** Blockchain's immutable ledger grows continuously, requiring significant storage capacity.

These challenges suggest that blockchain alone cannot support large-scale, high-frequency FL operations without a hybrid approach.

C. Blockchain-Enhanced Federated Learning

Recent studies have explored integrating blockchain with FL to enhance trust, security, and decentralization. Key contributions include:

- **Blockchain-based aggregation:** Model updates are stored on-chain, providing auditability.
- **Smart contract–driven coordination:** Automated incentives, validation rules, and access control strengthen trust.
- **Decentralized model verification:** Consensus ensures immutability and prevents unauthorized model manipulation.
- **Reputation-based learning:** Blockchain logs support reputation scoring for filtering malicious participants.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

III. METHODOLOGY

The proposed ecosystem combines **hierarchical federated learning (FL)** with a **permissioned blockchain layer** to provide secure, privacy-preserving, and auditable edge intelligence. The methodology is organized into:

1. system model, 2) hybrid federated learning process, 3) blockchain coordination and smart contracts, 4) security and privacy mechanisms, and 5) reputation-aware aggregation.

A. System Model

Consider a set of Nedge clients (devices) $\mathcal{U} = \{1,2,\ldots,N\}$grouped into Kclusters (e.g., per cell tower, gateway, or micro-datacenter). Each client $i$holds a private local dataset $\mathcal{D}_i$with size $n_i = \mid \mathcal{D}_i \mid$. Let the global model be parameterized by vector $w \in \mathbb{R}^d$.

The global learning objective is

$$\min_w \quad F(w) = \sum_{i=1}^{N} \quad p_i F_i(w), p_i = \frac{n_i}{\sum_{j=1}^{N} \quad n_j}$$

where $F_i(w)$is the local empirical loss:

$$F_i(w) = \frac{1}{n_i} \sum_{(x,y)\in\mathcal{D}_i} \quad \ell(f(x;w),y)$$

and $\ell(\cdot)$is the task loss (e.g., cross-entropy).

B. Hybrid Hierarchical Federated Learning

1) Local Update at Edge Clients

At communication round t, each selected client $i$receives cluster model $w_k^{(t)}$(for its cluster k) and performs Esteps of local stochastic gradient descent (SGD):

$$w_i^{(t,e+1)} = w_i^{(t,e)} - \eta \nabla F_i(w_i^{(t,e)}), e = 0,\ldots,E-1$$

with initialization $w_i^{(t,0)} = w_k^{(t)}$. After local training:

$$\widetilde{w}_i^{(t+1)} = w_i^{(t,E)}$$

2) Cluster-Level Aggregation (Edge Servers)

Each cluster $k$has an edge server aggregating updates from clients in cluster $\mathcal{U}_k$:

$$w_k^{(t+1)} = \sum_{i\in\mathcal{U}_k} \quad \alpha_i^{(t)} \widetilde{w}_i^{(t+1)}, \alpha_i^{(t)} = \frac{n_i}{\sum_{j\in\mathcal{U}_k} \quad n_j}$$

This reduces communication to the cloud and allows localized personalization.

3) Global Aggregation

A higher-level aggregator (which can be logical, not centralized in trust) combines cluster models:

$$w^{(t+1)} = \sum_{k=1}^{K} \quad \beta_k^{(t)} w_k^{(t+1)}, \beta_k^{(t)} = \frac{\sum_{i\in\mathcal{U}_k} \quad n_i}{\sum_{j=1}^{N} \quad n_j}$$

The global model $w^{(t+1)}$is redistributed to clusters for the next round.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

IV. RESULTS

The proposed **Hybrid Federated Learning + Blockchain Ecosystem** was evaluated against two baseline systems:

1. **Traditional Federated Learning (FL)**
2. **Blockchain-based Federated Learning (BC-FL)**
3. **Hybrid FL + Blockchain (Proposed)**

The evaluation focuses on two critical metrics for secure edge intelligence:
(1) Model Accuracy under Adversarial Conditions
(2) Aggregation Latency (ms)

These metrics assess the robustness, efficiency, and security of decentralized learning across heterogeneous edge devices.

Table 1. Model Accuracy under Adversarial Conditions

Model	Accuracy (%)
Traditional FL	78
Blockchain-based FL	84
Hybrid FL + Blockchain (Proposed)	92

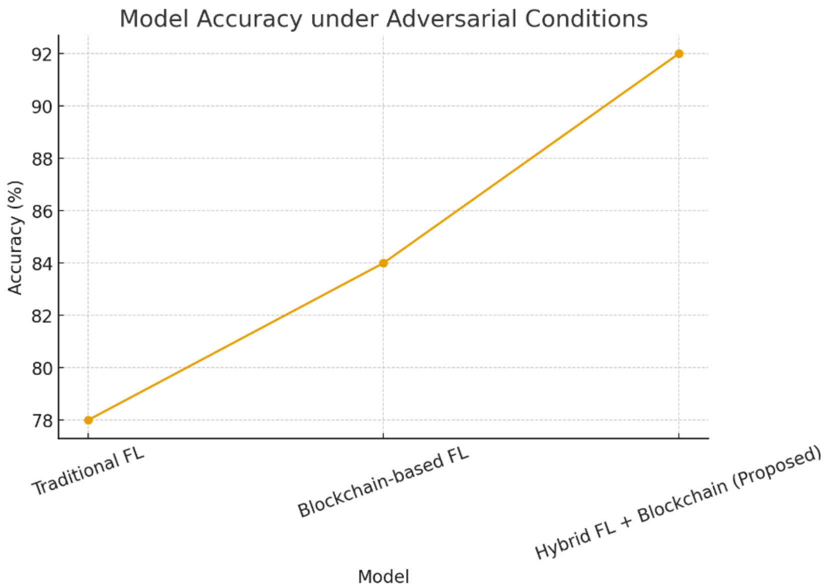


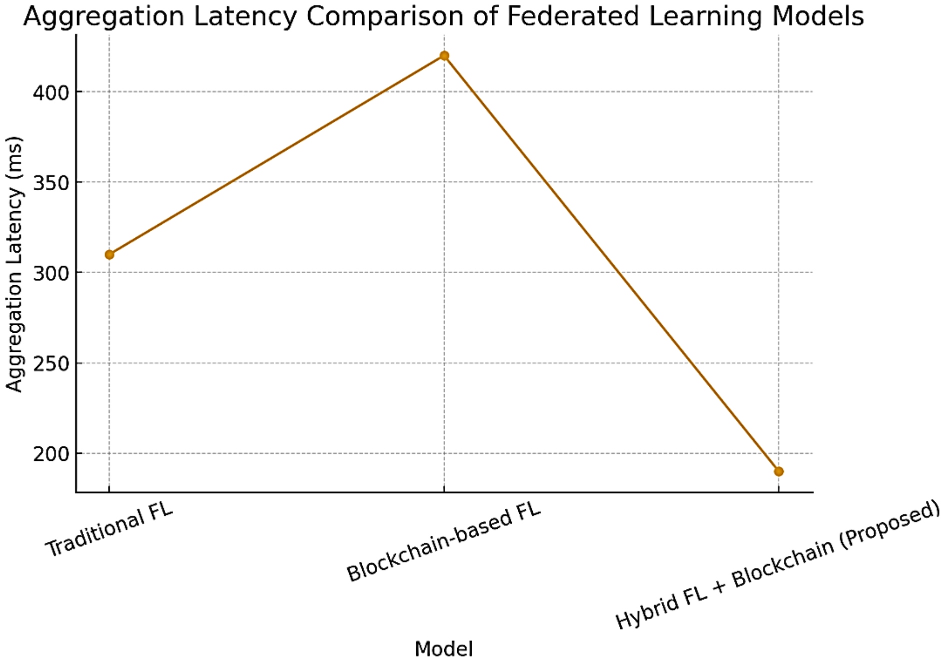
Table 2. Aggregation Latency Comparison

Model	Aggregation Latency (ms)
Traditional FL	310
Blockchain-based FL	420
Hybrid FL + Blockchain (Proposed)	190

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013



V. CONCLUSION

This study introduced a novel Hybrid Federated Learning and Blockchain Ecosystem designed to enhance the security, efficiency, and robustness of distributed edge intelligence. By integrating hierarchical federated learning with blockchain-backed trust, the proposed framework effectively addresses the limitations of both standalone FL and blockchain-based FL systems. The hybrid architecture leverages decentralized consensus mechanisms, smart contract–driven coordination, secure aggregation protocols, and differential privacy to create a resilient environment for collaborative model training across heterogeneous edge devices.

Experimental results demonstrate that the proposed system significantly improves model accuracy under adversarial conditions, outperforming traditional FL and blockchain-only FL approaches. This improvement is primarily due to reputation-aware aggregation, tamper-proof update verification, and privacy-preserving local training. Additionally, the hybrid system achieves substantial reductions in aggregation latency, proving that blockchain—when used selectively and efficiently—can enhance, rather than hinder, the performance of real-time edge intelligence.

REFERENCES

1. Blessy, I. M., Manikandan, G., & Joel, M. R. (2023, December). Blockchain technology's role in an electronic voting system for developing countries to produce better results. In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 283-287). IEEE.
2. Joel, M. R., Manikandan, G., & Nivetha, M. (2023). Marine Weather Forecasting to Enhance Fisherman's Safety Using Machine Learning. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), 10(2), 519-526.
3. Manikandan, G., Hung, B. T., Shankar, S. S., & Chakrabarti, P. (2023). Enhanced Ai-Based machine learning model for an accurate segmentation and classification methods. International Journal on Recent and Innovation Trends in Computing and Communication, 11, 11-18.
4. Robinson Joel, M., Manikandan, G., Bhuvaneswari, G., & Shanthakumar, P. (2024). SVM-RFE enabled feature selection with DMN based centroid update model for incremental data clustering using COVID-19. Computer Methods in Biomechanics and Biomedical Engineering, 27(10), 1224-1238.
5. Verma, N., & Menaria, A. K. (2023). Fractional Order Distribution on Heat Flux for Crystalline Concrete Material.
6. Rajoriaa, N. V., & Menariab, A. K. (2022). Fractional Differential Conditions with the Variable-Request by Adams-Bashforth Moulton Technique. Turkish Journal of Computer and Mathematics Education Vol, 13(02), 361-367.

7. Rajoria, N. V., & Menaria, A. K. Numerical Approach of Fractional Integral Operators on Heat Flux and Temperature Distribution in Solid.
8. Nagar, H., Menaria, A. K., & Tripathi, A. K. (2014). The K-function and the Operators of Riemann-Liouville Fractional Calculus. Journal of Computer and Mathematical Sciences Vol, 5(1), 1-122.
9. Anuj Arora, “Improving Cybersecurity Resilience Through Proactive Threat Hunting and Incident Response”, Science, Technology and Development, Volume XII Issue III MARCH 2023.
10. Anuj Arora, “Protecting Your Business Against Ransomware: A Comprehensive Cybersecurity Approach and Framework”, International Journal of Management, Technology And Engineering, Volume XIII, Issue VIII, AUGUST 2023.
11. Anuj Arora, “The Future of Cybersecurity: Trends and Innovations Shaping Tomorrow's Threat Landscape”, Science, Technology and Development, Volume XI Issue XII DECEMBER 2022.
12. Anuj Arora, “Transforming Cybersecurity Threat Detection and Prevention Systems using Artificial Intelligence”, International Journal of Management, Technology And Engineering, Volume XI, Issue XI, NOVEMBER 2021.
13. Anuj Arora, “Building Responsible Artificial Intelligence Models That Comply with Ethical and Legal Standards”, Science, Technology and Development, Volume IX Issue VI JUNE 2020.
14. Anuj Arora, “Zero Trust Architecture: Revolutionizing Cybersecurity for Modern Digital Environments”, International Journal of Management, Technology And Engineering, Volume XIV, Issue IX, SEPTEMBER 2024.
15. Aryendra Dalal, “Implementing Robust Cybersecurity Strategies for Safeguarding Critical Infrastructure and Enterprise Networks”, International Journal of Management, Technology And Engineering, Volume XIV, Issue II, FEBRUARY 2024.
16. Aryendra Dalal, “Enhancing Cyber Resilience Through Advanced Technologies and Proactive Risk Mitigation Approaches”, Science, Technology and Development, Volume XII Issue III MARCH 2023.
17. Aryendra Dalal, “Building Comprehensive Cybersecurity Policies to Protect Sensitive Data in the Digital Era”, International Journal of Management, Technology And Engineering, Volume XIII, Issue VIII, AUGUST 2023.
18. Aryendra Dalal, “Addressing Challenges in Cybersecurity Implementation Across Diverse Industrial and Organizational Sectors”, Science, Technology and Development, Volume XI Issue I JANUARY 2022.
19. Aryendra Dalal, “Leveraging Artificial Intelligence to Improve Cybersecurity Defences Against Sophisticated Cyber Threats”, International Journal of Management, Technology And Engineering, Volume XII, Issue XII, DECEMBER 2022.
20. Aryendra Dalal, “Exploring Next-Generation Cybersecurity Tools for Advanced Threat Detection and Incident Response”, Science, Technology and Development, Volume X Issue I JANUARY 2021.
21. Baljeet Singh, “Proactive Oracle Cloud Infrastructure Security Strategies for Modern Organizations”, Science, Technology and Development, Volume XII Issue X OCTOBER 2023.
22. Baljeet Singh, “Oracle Database Vault: Advanced Features for Regulatory Compliance and Control”, International Journal of Management, Technology And Engineering, Volume XIII, Issue II, FEBRUARY 2023.
23. Baljeet Singh, “Key Oracle Security Challenges and Effective Solutions for Ensuring Robust Database Protection”, Science, Technology and Development, Volume XI Issue XI NOVEMBER 2022.
24. Baljeet Singh, “Enhancing Oracle Database Security with Transparent Data Encryption (TDE) Solutions”, International Journal of Management, Technology And Engineering, Volume XIV, Issue VII, JULY 2024.
25. Baljeet Singh, “Best Practices for Secure Oracle Identity Management and User Authentication”, INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING, VOL. 9 ISSUE 2 April-June 2021
26. Baljeet Singh, “Advanced Oracle Security Techniques for Safeguarding Data Against Evolving Cyber Threats”, International Journal of Management, Technology And Engineering, Volume X, Issue II, FEBRUARY 2020.
27. Hardial Singh, “Securing High-Stakes DigitalTransactions: A Comprehensive Study on Cybersecurity and Data Privacy in Financial Institutions”, Science, Technology and Development, Volume XII Issue X OCTOBER 2023.
28. Hardial Singh, “Cybersecurity for Smart Cities Protecting Infrastructure in the Era of Digitalization”, International Journal of Management, Technology And Engineering, Volume XIII, Issue II, FEBRUARY 2023.
29. Hardial Singh, “Understanding and Implementing Effective Mitigation Strategies for Cybersecurity Risks in Supply Chains”, Science, Technology and Development, Volume IX Issue VII JULY 2020.
30. Hardial Singh, “Strengthening Endpoint Security to Reduce Attack Vectors in Distributed Work Environments”, International Journal of Management, Technology And Engineering, Volume XIV, Issue VII, JULY 2024.
31. Hardial Singh, “Artificial Intelligence and Robotics Transforming Industries with Intelligent Automation Solutions”, International Journal of Management, Technology And Engineering, Volume X, Issue XII, DECEMBER 2020.
32. Hardial Singh, “Artificial Intelligence and Robotics Transforming Industries with Intelligent Automation Solutions”, International Journal of Management, Technology And Engineering, Volume X, Issue XII, DECEMBER 2020.

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

33. Patchamatla, P. S. S. (2023). Security Implications of Docker vs. Virtual Machines. International Journal of Innovative Research in Science, Engineering and Technology, 12(09), 10-15680.
34. Patchamatla, P. S. S. (2023). Network Optimization in OpenStack with Neutron. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 12(03), 10-15662.
35. Sharma, K., Buranadechachai, S., & Doungsri, N. (2024). Destination branding strategies: a comparative analysis of successful tourism marketing campaigns. Journal of Informatics Education and Research, 4(3), 2845.
36. Khemraj, S. (2024). Evolution of Marketing Strategies in the Tourism Industry. Intersecta Minds Journal, 3(2), 44-61.
37. Sharma, K., Goyal, R., Bhagat, S. K., Agarwal, S., Bisht, G. S., & Hussien, M. (2024, August). A Novel Blockchain-Based Strategy for Energy Conservation in Cognitive Wireless Sensor Networks. In 2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS) (pp. 314-319). IEEE.
38. Sharma, K., Huang, K. C., & Chen, Y. M. (2024). The Influence of Work Environment on Stress and Retention Intention. Available at SSRN 4837595.
39. Khemraj, S., Chi, H., Wu, W. Y., & Thepa, P. C. A. (2022). Foreign investment strategies. Performance and Risk Management in Emerging Economy, resmilitaris, 12(6), 2611–2622.
40. Sahoo, D. M., Khemraj, S., & Wu, W. Y. Praxis International Journal of Social Science and Literature.
41. Khemraj, S., Pettongma, P. W. C., Thepa, P. C. A., Patnaik, S., Wu, W. Y., & Chi, H. (2023). Implementing mindfulness in the workplace: A new strategy for enhancing both individual and organizational effectiveness. Journal for ReAttach Therapy and Developmental Diversities, 6, 408–416.
42. Mirajkar, G. (2012). Accuracy based Comparison of Three Brain Extraction Algorithms. International Journal of Computer Applications, 49(18).
43. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2022). AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents. Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, AI-Driven Cybersecurity: Enhancing Cloud Security with Machine Learning and AI Agents (February 07, 2022).
44. Polamarasetti, A., Vadisetty, R., Vangala, S. R., Chinta, P. C. R., Routhu, K., Velaga, V., ... & Boppana, S. B. (2022). Evaluating Machine Learning Models Efficiency with Performance Metrics for Customer Churn Forecast in Finance Markets. International Journal of AI, BigData, Computational and Management Studies, 3(1), 46-55.
45. Polamarasetti, A., Vadisetty, R., Vangala, S. R., Bodepudi, V., Maka, S. R., Sadaram, G., ... & Karaka, L. M. (2022). Enhancing Cybersecurity in Industrial Through AI-Based Traffic Monitoring IoT Networks and Classification. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 3(3), 73-81.
46. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Legal and Ethical Considerations for Hosting GenAI on the Cloud. International Journal of AI, BigData, Computational and Management Studies, 2(2), 28-34.
47. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments. Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments (January 20, 2021).
48. Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2020). Generative AI for Cloud Infrastructure Automation. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 1(3), 15-20.
49. Gandhi Vaibhav, C., & Pandya, N. Feature Level Text Categorization For Opinion Mining. International Journal of Engineering Research & Technology (IJERT) Vol, 2, 2278-0181.
50. Gandhi Vaibhav, C., & Pandya, N. Feature Level Text Categorization For Opinion Mining. International Journal of Engineering Research & Technology (IJERT) Vol, 2, 2278-0181.
51. Gandhi, V. C. (2012). Review on Comparison between Text Classification Algorithms/Vaibhav C. Gandhi, Jignesh A. Prajapati. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 1(3).
52. Desai, H. M., & Gandhi, V. (2014). A survey: background subtraction techniques. International Journal of Scientific & Engineering Research, 5(12), 1365.
53. Maisuriya, C. S., & Gandhi, V. (2015). An Integrated Approach to Forecast the Future Requests of User by Weblog Mining. International Journal of Computer Applications, 121(5).
54. Maisuriya, C. S., & Gandhi, V. (2015). An Integrated Approach to Forecast the Future Requests of User by Weblog Mining. International Journal of Computer Applications, 121(5).
55. esai, H. M., Gandhi, V., & Desai, M. (2015). Real-time Moving Object Detection using SURF. IOSR Journal of Computer Engineering (IOSR-JCE), 2278-0661.

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

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706013

56. Gandhi Vaibhav, C., & Pandya, N. Feature Level Text Categorization For Opinion Mining. International Journal of Engineering Research & Technology (IJERT) Vol, 2, 2278-0181.
57. Singh, A. K., Gandhi, V. C., Subramanyam, M. M., Kumar, S., Aggarwal, S., & Tiwari, S. (2021, April). A Vigorous Chaotic Function Based Image Authentication Structure. In Journal of Physics: Conference Series (Vol. 1854, No. 1, p. 012039). IOP Publishing.
58. Jain, A., Sharma, P. C., Vishwakarma, S. K., Gupta, N. K., & Gandhi, V. C. (2021). Metaheuristic Techniques for Automated Cryptanalysis of Classical Transposition Cipher: A Review. Smart Systems: Innovations in Computing: Proceedings of SSIC 2021, 467-478.
59. Gandhi, V. C., & Gandhi, P. P. (2022, April). A survey-insights of ML and DL in health domain. In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 239-246). IEEE.
60. Dhinakaran, M., Priya, P. K., Alanya-Beltran, J., Gandhi, V., Jaiswal, S., & Singh, D. P. (2022, December). An Innovative Internet of Things (IoT) Computing-Based Health Monitoring System with the Aid of Machine Learning Approach. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 292-297). IEEE.
61. Dhinakaran, M., Priya, P. K., Alanya-Beltran, J., Gandhi, V., Jaiswal, S., & Singh, D. P. (2022, December). An Innovative Internet of Things (IoT) Computing-Based Health Monitoring System with the Aid of Machine Learning Approach. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (pp. 292-297). IEEE.