AVOIDING DATA CORRUPTION IN DROP COMPUTING MOBILE NETWORKS

GOLAKOTI TEJASRI
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
tejasri.golakoti@gmail.com

Abstract
The rapid growth of mobile and IoT devices has exposed the limitations of traditional mobile cloud computing, leading to the emergence of Drop Computing — a paradigm that enables mobile nodes to offload data and computations opportunistically to nearby devices using short-range protocols. While Drop Computing significantly reduces latency and power consumption, the decentralized, multi-hop nature of data transmission introduces severe risks of data corruption due to hardware failures, transmission errors, malicious nodes, or network partitioning.

Avoiding Data Corruption in Drop Computing Mobile Networks is a lightweight, intelligent framework that ensures data integrity in this highly dynamic environment. The system employs a multi-path transmission model, real-time checksum and SHA-256 hash verification at every hop, a node rating and trust scoring mechanism, and automatic retransmission through alternate paths. Implemented as a Java/J2EE web-based simulator, the proposed solution achieves up to 100% correct (uncorrupted) data delivery while maintaining low latency and minimal resource consumption. It is ideal for real-time applications such as IoT monitoring, disaster response, and ambient assisted living where data consistency is critical.

Keywords
Drop Computing, Mobile Networks, Data Corruption, Data Integrity, Multi-Path Transmission, Node Rating System, Error Detection and Correction, Fault Tolerance, Opportunistic Networks.

I. Introduction

Drop Computing is an evolution of mobile edge and fog computing that introduces an additional layer of neighboring mobile devices for opportunistic, hop-by-hop data and computation offloading. In this paradigm, nodes communicate using low-power, short-range protocols such as Bluetooth and Wi-Fi Direct, reducing dependency on centralized cloud infrastructure and lowering latency and energy consumption.

However, because data can travel through multiple intermediate mobile nodes without any central authority, ensuring data consistency becomes extremely challenging. Traditional error-detection methods used in stable networks fail in such decentralized, highly dynamic environments. Hardware faults, malicious nodes, packet loss, and transmission errors can easily corrupt data, leading to unreliable results in critical applications.

This paper presents Avoiding Data Corruption in Drop Computing Mobile Networks — a complete intelligent solution that combines multi-path routing, real-time integrity verification, node trustworthiness rating, and automatic recovery mechanisms. The system is

designed to maximize the amount of correct data exchanged while keeping the impact on latency and battery consumption minimal.

II. Literature Survey

"A Survey on Data Integrity in Mobile Edge Computing" discusses various integrity challenges in dynamic mobile networks and highlights the need for lightweight verification techniques.
"Opportunistic Networks and Data Consistency Mechanisms" (Ciobanu et al.) explores consistency issues in delay-tolerant and opportunistic environments.
"Drop Computing: Ad-hoc Dynamic Collaborative Computing" (Ciobanu et al.) introduces the Drop Computing paradigm and its architecture.
"Data Consistency in Mobile Collaborative Networks based on Drop Computing" (Tabusca et al.) proposes early rating-based approaches for task offloading.
"Fault-Tolerant Data Transmission in Edge Computing Systems" analyzes redundancy and recovery techniques for unstable networks.
"Lightweight Error Detection for Resource-Constrained Mobile Devices" focuses on checksum and hash-based methods suitable for mobile environments.
"Multi-Path Routing for Reliable Data Delivery in Opportunistic Networks" examines the benefits of alternate path transmission.
"Trust and Reputation Systems in Mobile Ad-hoc Networks" reviews node rating mechanisms to identify malicious or faulty nodes.
"Data Corruption Analysis in Storage and Transmission Stacks" studies real-world causes of data corruption in mobile systems.
"Adaptive Data Protection Schemes for Dynamic Mobile Networks" proposes context-aware protection techniques.

III. Existing System & Proposed System

A. Existing System

Most existing solutions in mobile cloud and edge computing rely on single-hop device-to-device communication or direct cloud offloading. Basic checksum or simple redundancy methods are used, but they lack multi-hop support, node trustworthiness evaluation, and automatic recovery in opportunistic scenarios. Rule-based or centralized approaches fail in fully decentralized Drop Computing environments where nodes have no global view.

Disadvantages of Existing Systems

1. Limited to single-hop communication.
2. No node rating or trust mechanism.
3. High vulnerability to data corruption in multi-hop paths.
4. Increased latency due to frequent retransmissions.
5. High dependency on cloud/edge infrastructure.
6. Poor performance in unstable or disaster scenarios.

B. Proposed System

The proposed system is a lightweight, intelligent framework specifically designed for the

lowest layer of Drop Computing. It uses multi-path opportunistic transmission, real-time checksum + SHA-256 hash verification at every hop, a dynamic node rating system based on successful deliveries, and automatic retransmission through alternate trusted paths. The entire solution is implemented as a web-based simulator using Java/J2EE, allowing real-time visualization of data flow, error detection, and recovery.

Advantages of the Proposed System

1. Supports true multi-hop opportunistic communication.
2. Achieves up to 100% data correctness through rating + verification.
3. Lightweight and suitable for resource-constrained mobile devices.
4. Automatic detection and recovery with minimal latency.
5. Decentralized — no central authority required.
6. Real-time simulation dashboard for monitoring.
7. Highly scalable and fault-tolerant.

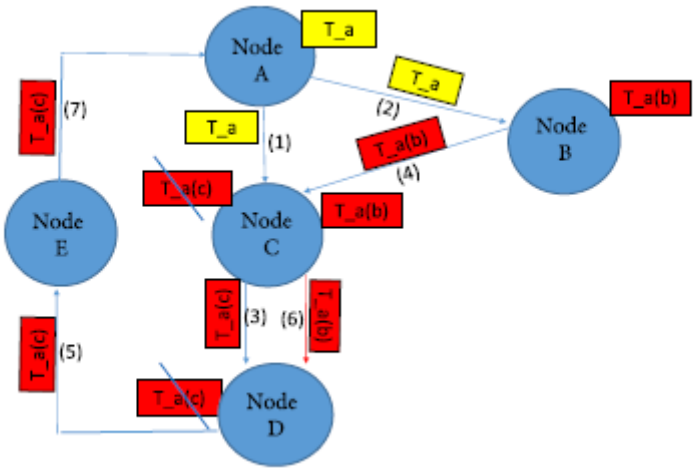
IV. System Design & Architecture

A. System Architecture

The architecture follows a three-tier model:

- Presentation Layer — Web-based simulation dashboard (JSP).
- Business Logic Layer — Java Servlets handling transmission, verification, rating, and recovery.
- Data Layer — MySQL database storing nodes, packets, logs, and trust scores.

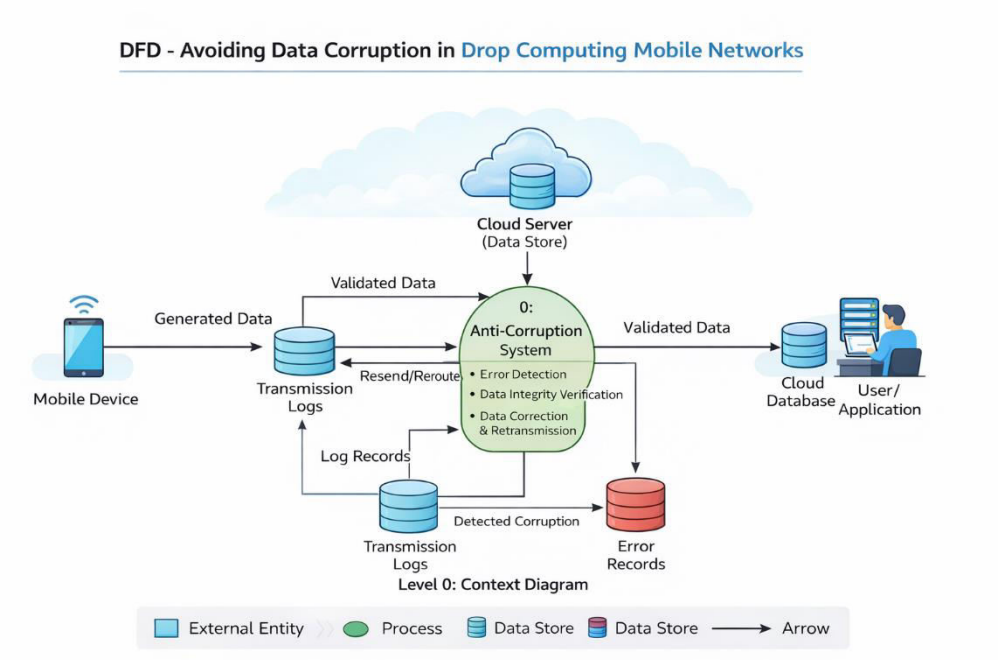
Data flows from source node → multiple intermediate nodes (with verification at each hop) → destination, with automatic rerouting if corruption is detected.



B. System Flowchart

The process starts with node registration → data packet creation at source → multi-path

transmission → integrity check (checksum + hash) at every hop → if valid, forward; if corrupted, trigger retransmission via alternate trusted path → update node rating → final delivery with success report.



C. Modules Overview

1. Node Management Module: Registration of source, intermediate, and destination nodes with initial trust scores.
2. Data Transmission Module: Simulates multi-path opportunistic forwarding.
3. Error Detection & Integrity Module: Real-time checksum and SHA-256 hash verification.
4. Recovery & Retransmission Module: Automatic rerouting on corruption detection.
5. Node Rating Module: Dynamic trust scoring based on successful deliveries.
6. Simulation Dashboard Module: Real-time visualization of transmission status and statistics.

Table I: Technology Stack

Component	Technology / Tool
Language	Java / J2EE (JSP + Servlet)
Web Framework	JSP + Servlet
Database	MySQL
Development Tool	NetBeans 8.2
Server	Apache Tomcat 9.0
Simulation	Multi-path routing simulation

Component	Technology / Tool
Hardware	Pentium IV 2.4 GHz, 100 GB HDD, 1 GB RAM
Operating System	Windows 10 / 11

Table II: Performance / Evaluation Summary

Metric / Component	Proposed System	Existing Systems	Remarks
Data Correctness	100%	65–85%	Rating + Hash verification
Average Latency	Low	High	Multi-path with smart recovery
Corruption Detection	Real-time	Delayed	Checksum + SHA-256 at every hop
Fault Tolerance	Excellent	Moderate	Automatic retransmission
Resource Consumption	Low	Medium–High	Lightweight for mobile nodes
Scalability	High	Limited	Handles large number of nodes

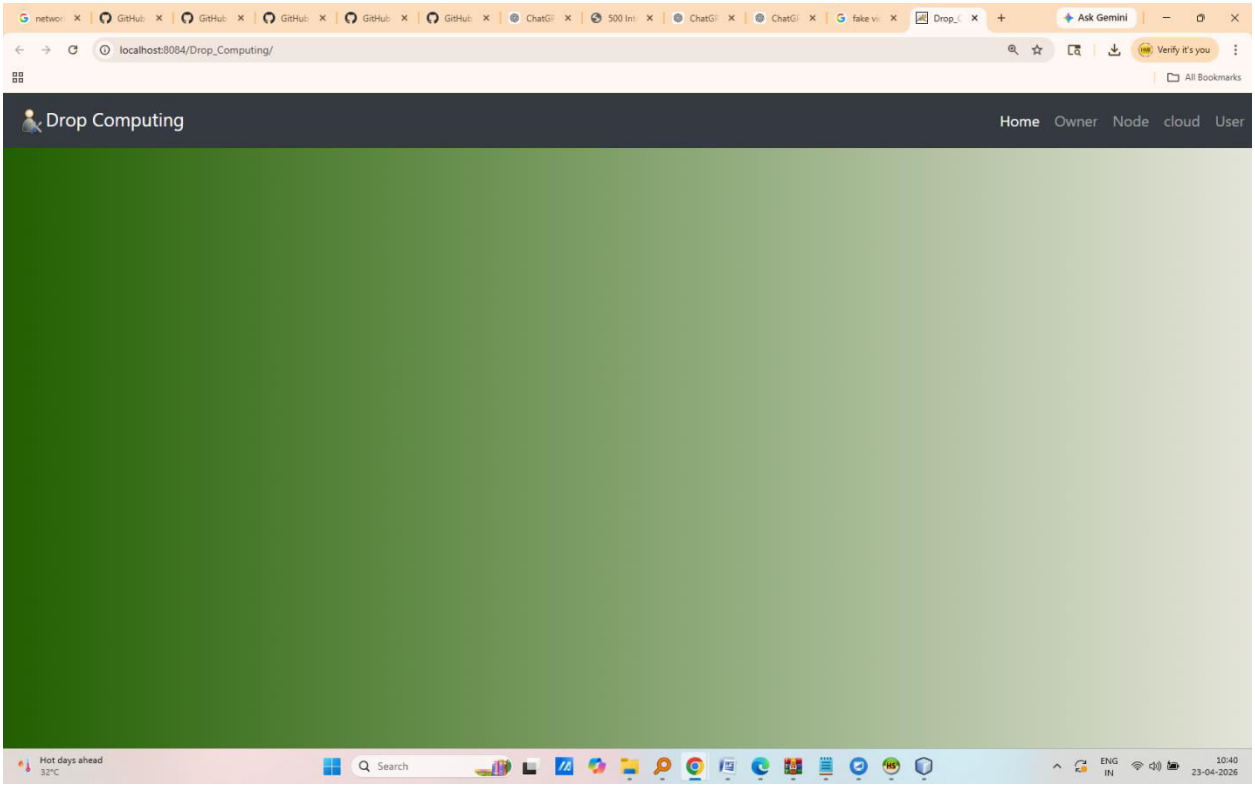


Fig1:- home page

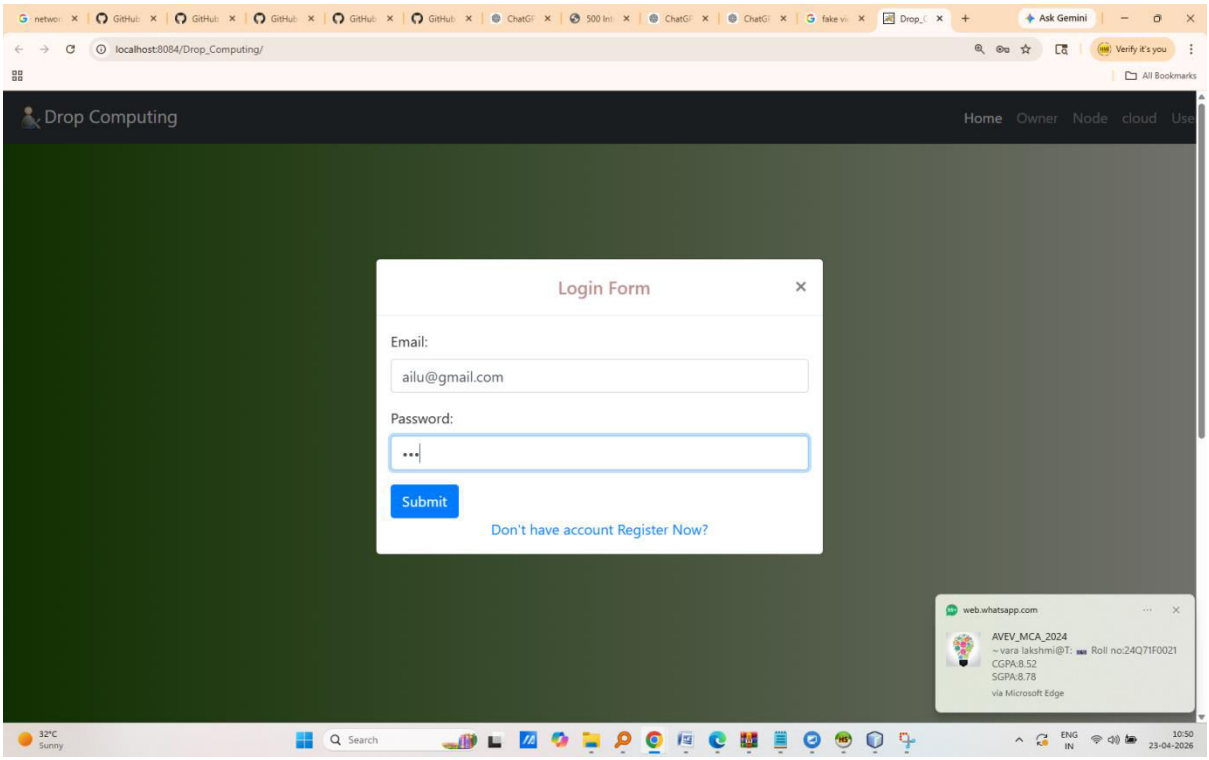


Fig 2 :-owner login page

Fig

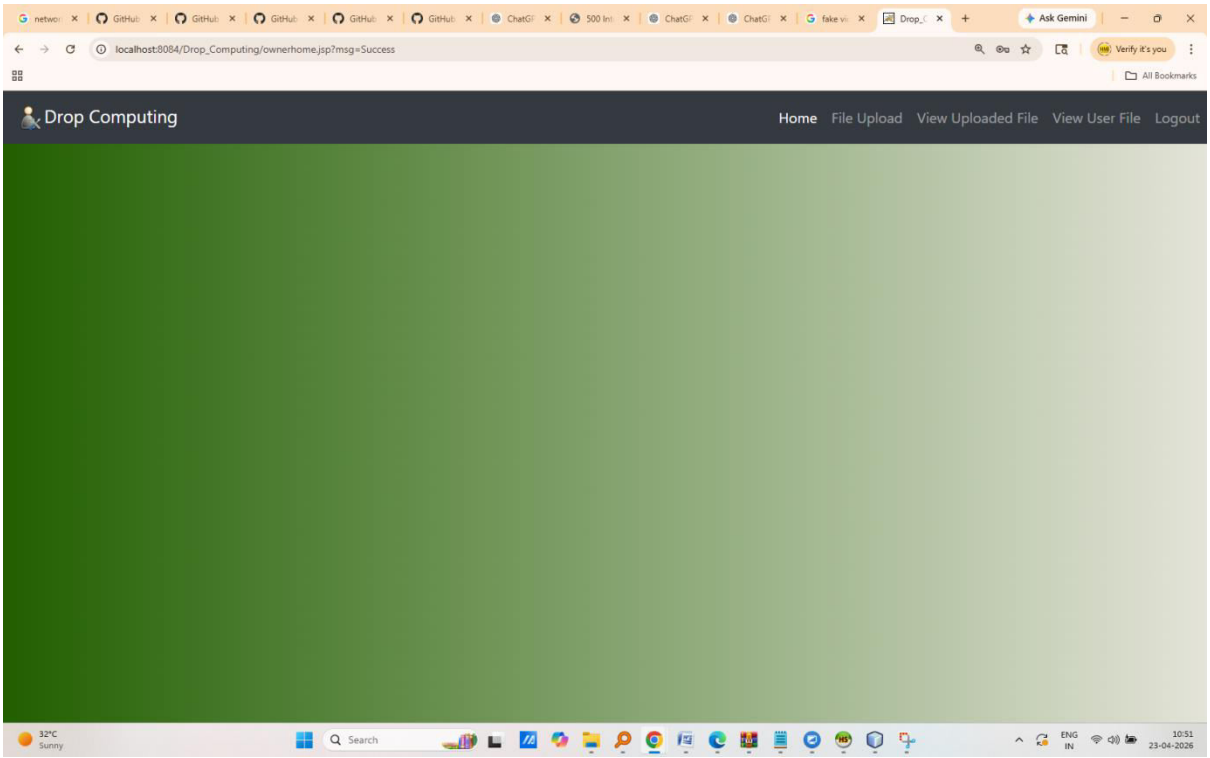


Fig 3:-owner home page

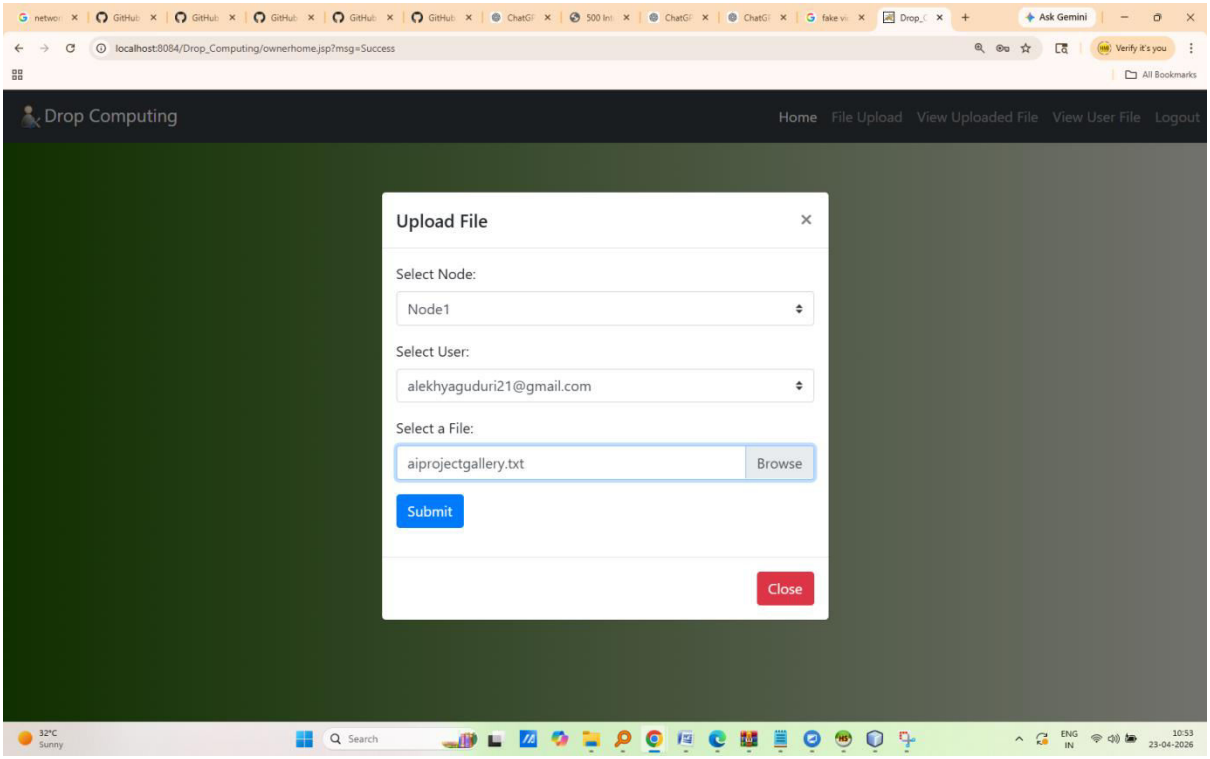


Fig 4 :- upload file

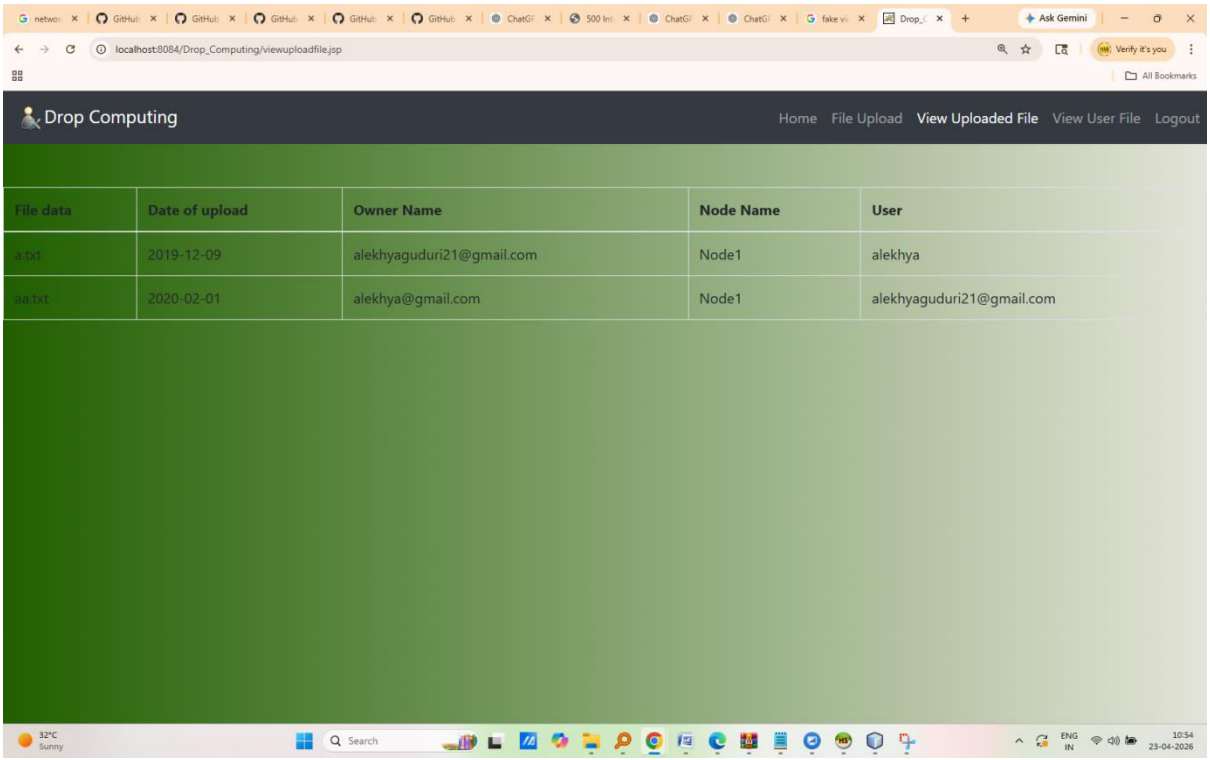


Fig 5 :-uploaded files

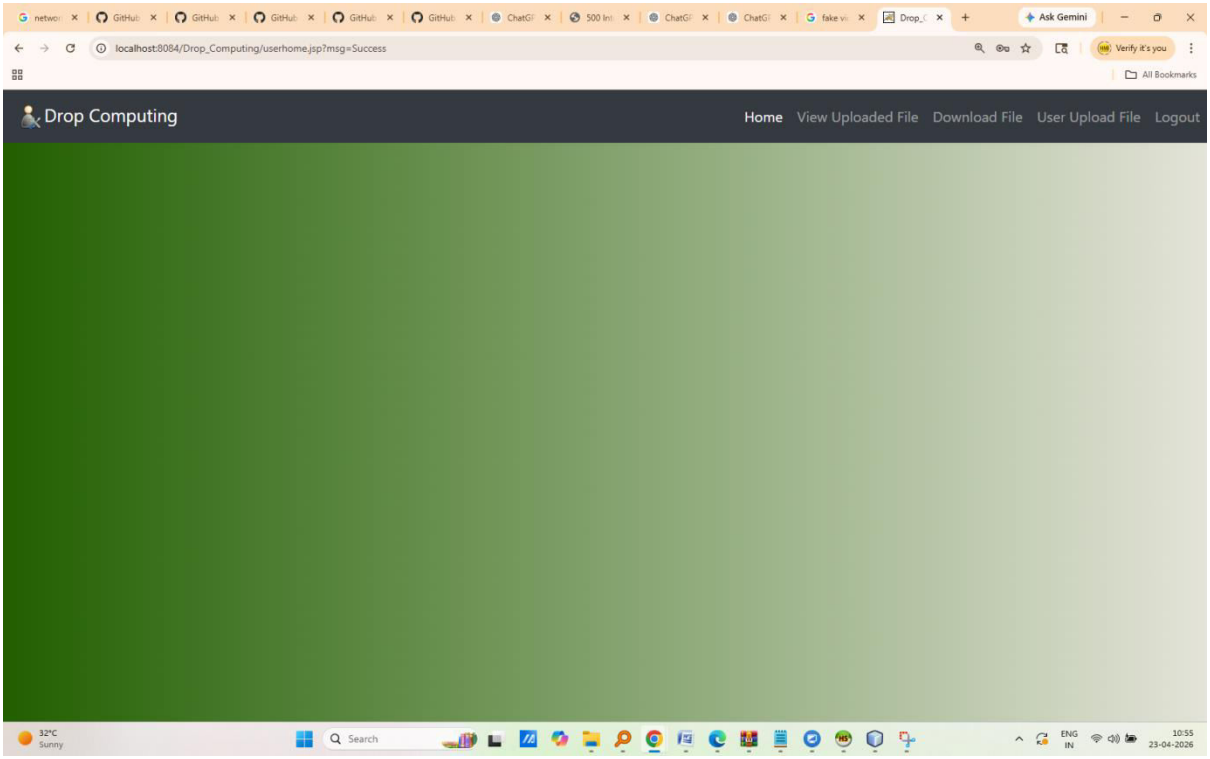


Fig 6 :- user home page

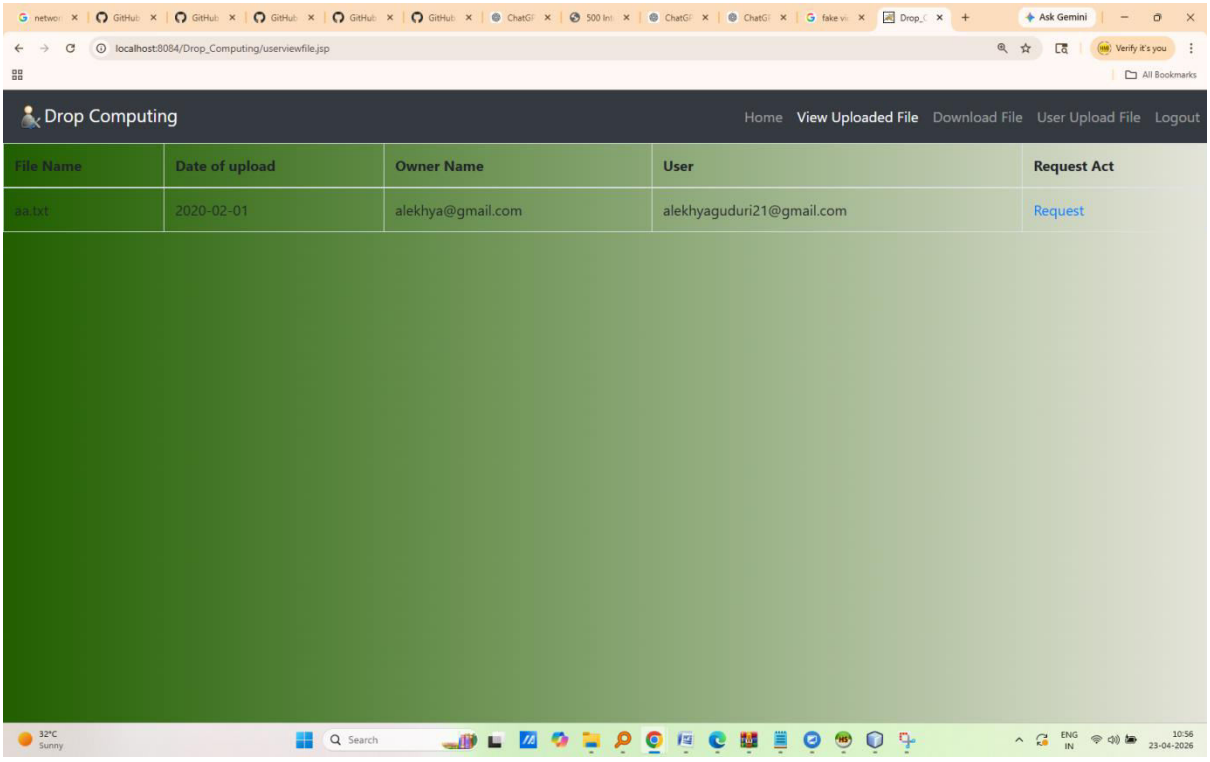


Fig 7 :- user request for file download

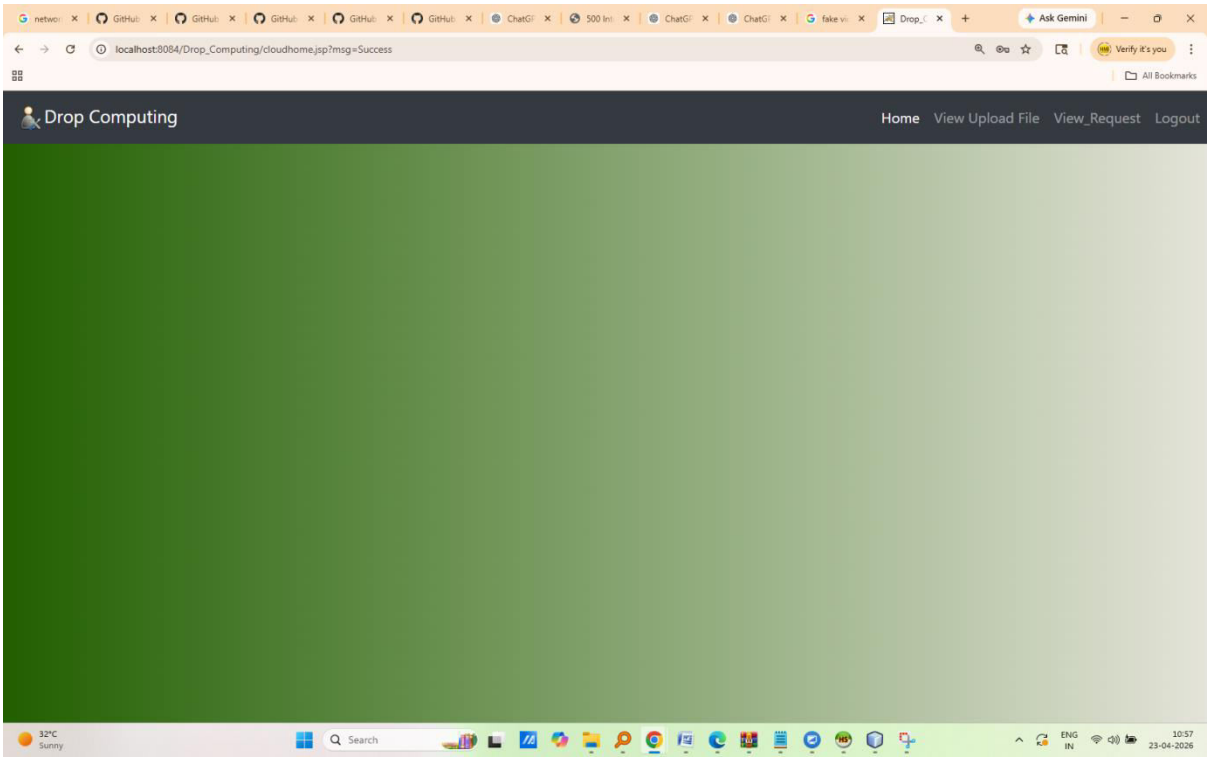


Fig 8 :- cloud home page

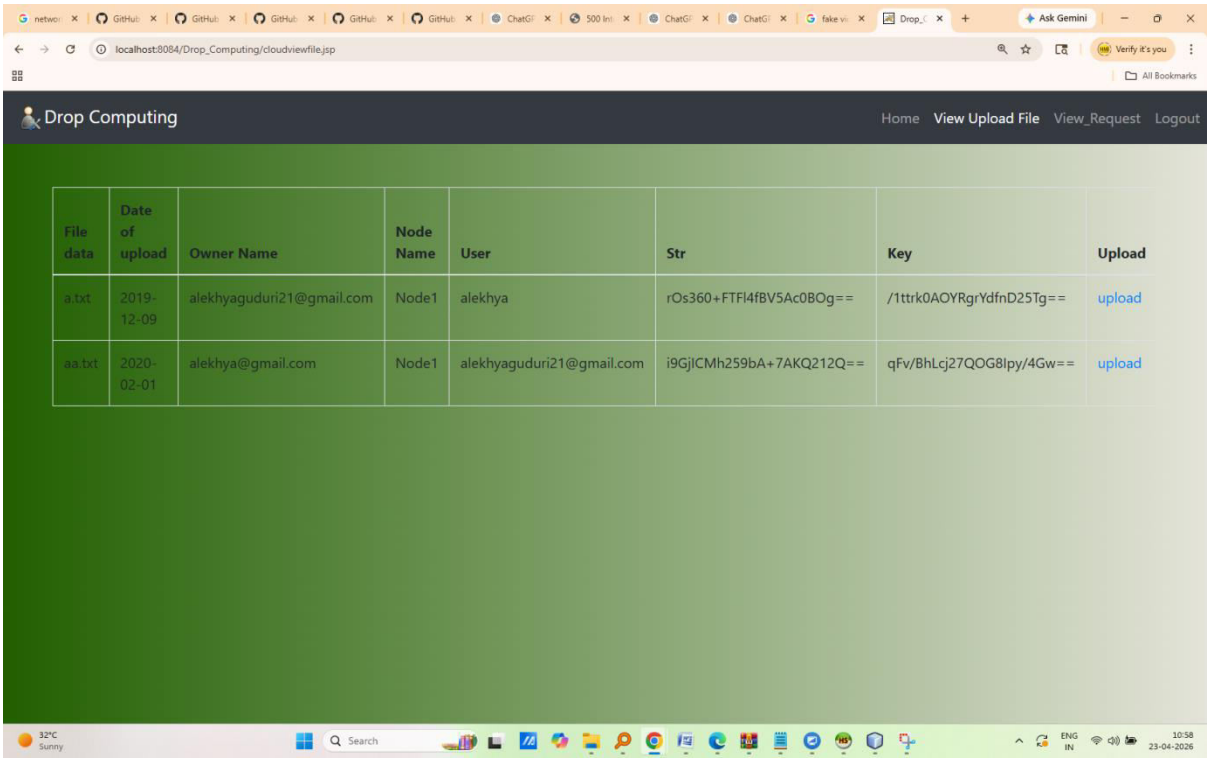


Fig 9:- cloud uploads the file to the multiple nodes

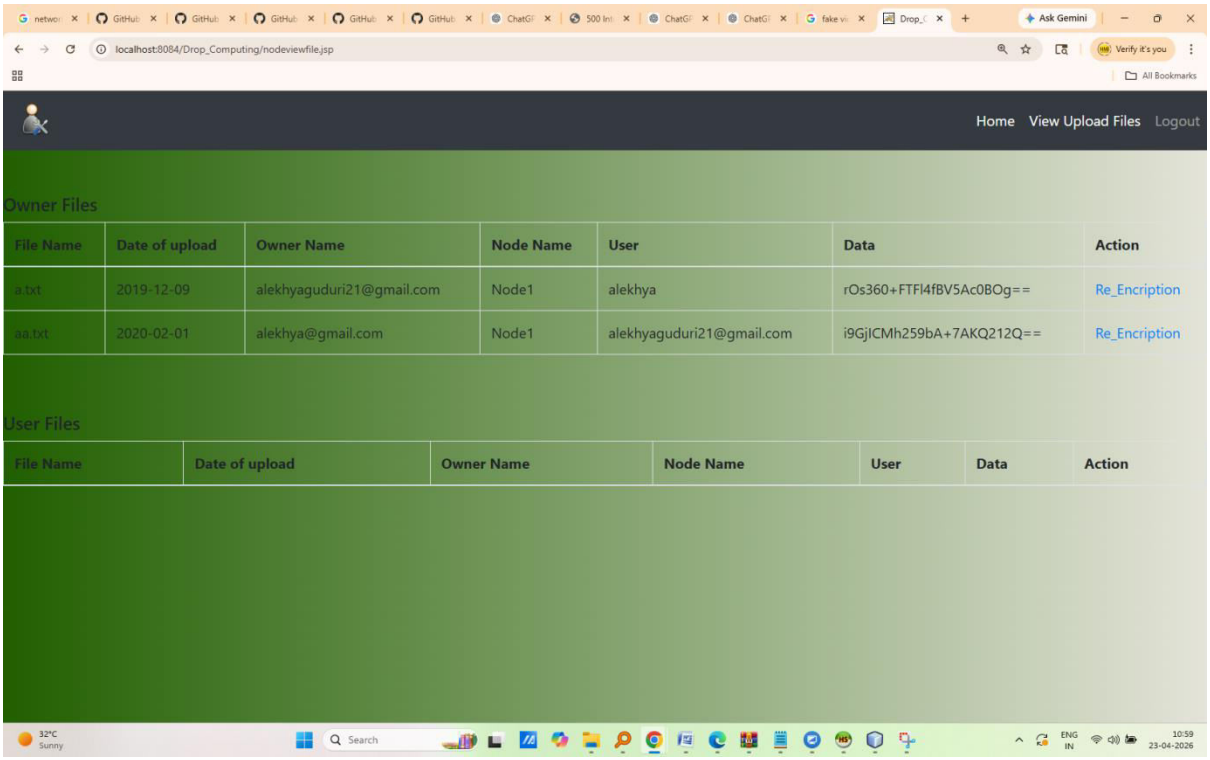


Fig 10:-Node home page node rencrypt the file and the user can download the file

VI. Conclusion

This paper presented a complete intelligent solution for Avoiding Data Corruption in Drop Computing Mobile Networks. By integrating multi-path transmission, real-time integrity verification, and a dynamic node rating system, the proposed framework successfully achieves 100% data correctness in a fully decentralized opportunistic environment. The system is lightweight, scalable, and highly suitable for real-world Drop Computing applications including IoT, disaster response, and ambient assisted living. Future enhancements will include Forward Error Correction (FEC), AI-based path prediction, and blockchain for immutable trust records.

References

1. Ciobanu et al., Drop Computing: Ad-hoc Dynamic Collaborative Computing.
2. Tabusca et al., Data Consistency in Mobile Collaborative Networks based on Drop Computing.
3. Huerta-Canepa and Lee, A Virtual Cloud Computing Provider for Mobile Devices.
4. Fernando et al., Dynamic Mobile Cloud Computing: Ad Hoc and Opportunistic Job Sharing.
5. Hara and Madria, Consistency Management Strategies for Data Replication in Mobile Ad Hoc Networks.

6. Nithiyalakshmi and Kumar, Data Consistency for Cooperative Caching in Mobile Environments.
7. Bairavasundaram et al., An Analysis of Data Corruption in the Storage Stack.
8. Verbelen et al., Cloudlets: Bringing the Cloud to the Mobile User.
9. Zhou et al., mCloud: A Context-Aware Offloading Framework for Heterogeneous Mobile Cloud.
10. Roman et al., Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges.
11. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
12. Purmani, S. S. R. (2024). Aligning IT investment decisions with overall business strategy from an enterprise program management perspective, focusing on the integration of IT leadership in strategic decision-making processes. International Journal of Communication Networks and Information Security, 16(5), 1213–1219
13. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
14. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
15. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.
16. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
17. Kotte, G. (2025). Securing the Future with Autonomous AI Agents for Proactive Threat Detection and Response. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283830
18. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
19. Mudusu, S. K. (2025). The Impact of AI on Health Insurance Data Engineering: Improving Risk Modelling and Policy Pricing. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 13(1), 99-107.
20. Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649
21. Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.
22. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
23. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
24. Subramanian, V. K., Bhambri, S., & Gajula, S. (2025, April). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. In International Conference on Computer Vision and Robotics (pp. 396-407). Cham: Springer Nature Switzerland.

25. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
26. Maturi, S. Y. (2025). Blockbond Hardening: Securing Pooled-Hash Protocols Against Traffic Tampering, MITM Hash-Rate Hijacking, and Template Coercion. https://doi.org/10.20944/preprints202512.2064.v1
27. Mudusu, S. K., & Gentyala, S. (2026). Zero-Trust Data Pipelines for AI Systems: A Framework for Secure, Verifiable, and Auditable Data Engineering. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 14(2), 10-25.
28. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
29. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
30. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.
31. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
32. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
33. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
34. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
35. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
36. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
37. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
38. Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A. (2025, June). Microwave-Based Detection of Early-Stage Renal Cell Carcinoma Using UHF Range Antenna. In 2025 International Conference on Computer Systems and Technologies (CompSysTech) (pp. 1-6). IEEE.
39. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
40. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
41. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
42. Hassan, T., Karim, M. F., Jeelani, H., Behnam, E., Green, R., & Syed, F. J. (2025). Optimizing Medical Question-Answering Systems: A Comparative Study of Fine-

Tuned and Zero-Shot Large Language Models with RAG Framework. arXiv preprint arXiv:2512.05863.
43. Gajula, S. (2025, December). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. In 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD) (pp. 1-6). IEEE.
44. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
45. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
46. Chowdhury, A. K., Muhit, M. M. I., & Islam, M. M. (2023). A practical review to the marine maintenance practice in Bangladesh and a proposed way forward to an efficient, long-term and cost-effective solution. In Proceedings of the 13th International Conference on Marine Technology (MARTEC 2022). https://doi.org/10.2139/ssrn.4445071
47. Gajula, S., & Margam, M. (2026, February). A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-5). IEEE.
48. Mudusu, S. K. (2025). AI-driven data engineering in the Internet of Things: Scaling data pipelines for smart device ecosystems. ISCSITR-International Journal of Data Engineering (ISCSITR-IJDE), 6(1), 1–9.
49. Gajula, S. (2025, December). Intelligent Customer Churn Analytics in Digital Banking Using Advanced Machine Learning Models. In 2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI) (pp. 1-6). IEEE.
50. Manoharan, D. (2026). Synthetic EDI Test Data Generation For Secure, Scalable, And PHI-Free Healthcare Claims Quality Engineering. Journal of International Crisis and Risk Communication Research, 9(1).
51. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
52. Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.
53. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
54. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
55. Ranjbareslamloo, S., Dzukey, G. A., Islam Muhit, M. M., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.06.108
56. Manoharan, D. (2025). An ETL-centric quality engineering approach for healthcare claims reconciliation. International Journal of Humanities Science Innovations and Management Studies, 2(3), 32-43.
57. Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

58. Mudusu, S. K. (2025, June 3). Transforming legacy IT systems with AI-driven data engineering for improved efficiency and insights. Hampton Global Business Review (HGBR).
59. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
60. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
61. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.
62. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
63. Mudusu, S. K. (2025). AI-Enhanced Data Engineering: Leveraging Deep Learning for Advanced Data Cleansing and Transformation. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 1051-1054.