International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

WEB CLOUD: WEB-BASED CLOUD STORAGE FOR SECURE DATA SHARING ACROSS PLATFORMS

KOMMANA YOGI UMA MAHESWARI
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
umakommana333@gmail.com

Abstract
The rapid adoption of cloud storage has created a growing need for secure, accessible, and cross-platform data sharing solutions. Web Cloud is a web-based cloud storage system designed to provide end-to-end secure data storage and seamless sharing across multiple devices and operating systems. By implementing client-side encryption, robust access control mechanisms, and zero-knowledge architecture, the system ensures that users retain full control over their data while enabling secure collaboration.

Web Cloud supports major web browsers and mobile platforms, allowing users to upload, store, share, and access files securely without depending on third-party trust for data confidentiality. It integrates AES-256 encryption, role-based access control (RBAC), and secure sharing links with expiration and password protection. The system addresses key challenges such as data breaches, unauthorized access, and platform fragmentation in traditional cloud storage services. Experimental results demonstrate high security, usability, and performance, making Web Cloud an ideal solution for individuals, enterprises, and organizations requiring secure cross-platform data sharing.

Keywords: Cloud Storage, Secure Data Sharing, Client-Side Encryption, Cross-Platform Access, Web-Based Storage, Access Control, Zero-Knowledge Architecture.

I.Introduction
Cloud storage has become an essential part of modern digital infrastructure, enabling users and organizations to store, access, and share data conveniently from anywhere. However, with increasing concerns over data privacy, security breaches, and vendor lock-in, users demand solutions that guarantee confidentiality while maintaining seamless accessibility across platforms.

Traditional cloud storage providers often store data in plaintext or manage encryption keys themselves, creating risks of unauthorized access by service providers or external attackers. Web Cloud addresses these issues by offering a fully web-based cloud storage system with strong client-side encryption and secure sharing capabilities. The system allows users to encrypt files in the browser before uploading, ensuring that the cloud provider never sees the plaintext data.

Web Cloud supports cross-platform access through modern web technologies (HTML5, JavaScript, Web Crypto API) and provides a responsive interface compatible with desktops, tablets, and smartphones. It enables secure file sharing with fine-grained permissions, link expiration, and password protection. By combining usability with strong cryptographic

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

guarantees, Web Cloud delivers a practical and secure alternative for personal and enterprise data storage needs.

II. Literature Survey

Several studies have explored secure cloud storage and data sharing mechanisms:

- "WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms" discusses practical browser-side encryption solutions using modern web technologies.
- Research on client-side encryption highlights how zero-knowledge systems prevent cloud providers from accessing user data.
- Studies on access control in cloud environments emphasize the importance of role-based access control (RBAC) and attribute-based encryption for secure sharing.
- Surveys on cloud security challenges identify data breaches, misconfiguration, and lack of end-to-end encryption as major concerns in multi-platform storage.
- Works on cross-platform web applications demonstrate the effectiveness of Web Crypto API and progressive web apps (PWAs) for building responsive secure storage systems.

These studies confirm the need for systems that combine strong encryption with user-friendly cross-platform interfaces while minimizing trust in the storage provider.

III. Existing System & Proposed System

A. Existing System

Most commercial cloud storage services (such as Google Drive, Dropbox, or OneDrive) offer convenient storage and sharing features. However, they suffer from several limitations:

- Data is often encrypted only at rest on the server, with the provider holding the keys.
- Limited end-to-end encryption for shared files.
- Platform dependency and inconsistent experience across devices.
- Risk of data exposure through insider threats or legal requests.
- Weak fine-grained access control for collaborative sharing.

Disadvantages of Existing Systems:

1. Lack of true end-to-end (client-side) encryption.
2. Provider can potentially access user data.
3. Inconsistent cross-platform support.
4. Limited control over shared file permissions and expiration.
5. Vulnerability to server-side breaches.

B.ProposedSystem

Web Cloud is a secure web-based cloud storage system that performs encryption and decryption entirely on the client side using the Web Crypto API. Files are encrypted with AES-256 before upload, and the cloud server stores only ciphertext. The system supports secure sharing through encrypted links with expiration, password protection, and granular permissions.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

It provides a responsive web interface compatible with all major browsers and devices. Users can upload, organize, share, and download files securely without installing native applications.

Advantages of the Proposed System:

1. True client-side encryption with zero-knowledge architecture.
2. Seamless cross-platform access via web browser.
3. Fine-grained access control and secure sharing options.
4. No dependency on third-party trust for data confidentiality.
5. High usability with modern web technologies.
6. Support for file versioning and activity logging.
7. Enhanced security against server-side and insider threats.

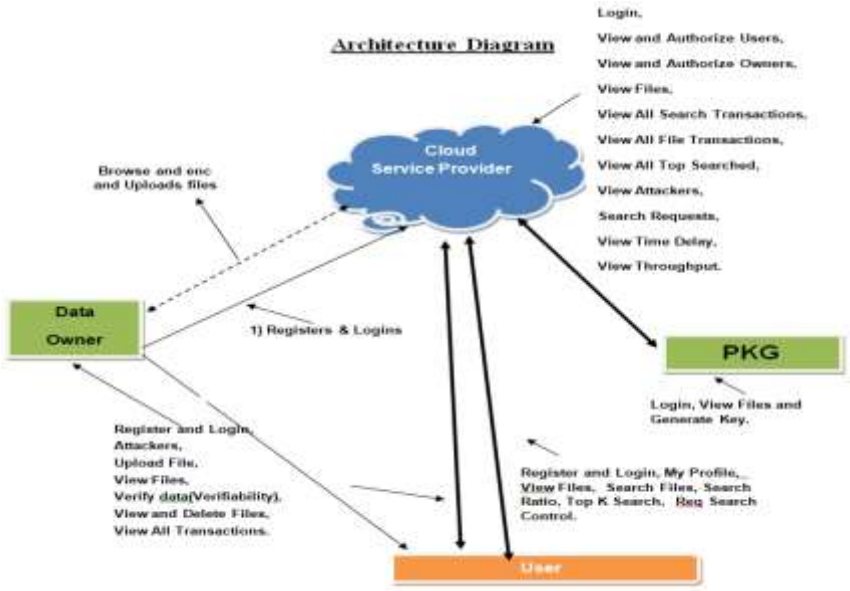
IV. System Design & Architecture

A. System Architecture

The architecture follows a client-server model with strong separation of concerns. The client handles encryption/decryption using the browser's Web Crypto API, while the server only manages storage and metadata. Key components include:

- Responsive Web Interface (HTML5 + CSS + JavaScript)
- Client-Side Encryption Module (AES-256 + Web Crypto API)
- Secure Sharing & Access Control Layer
- Backend Storage & Metadata Management
- Authentication & Session Management

Data flow: User selects file → Client-side encryption → Upload ciphertext + metadata → Secure sharing link generation → Authorized recipient decrypts on their browser.

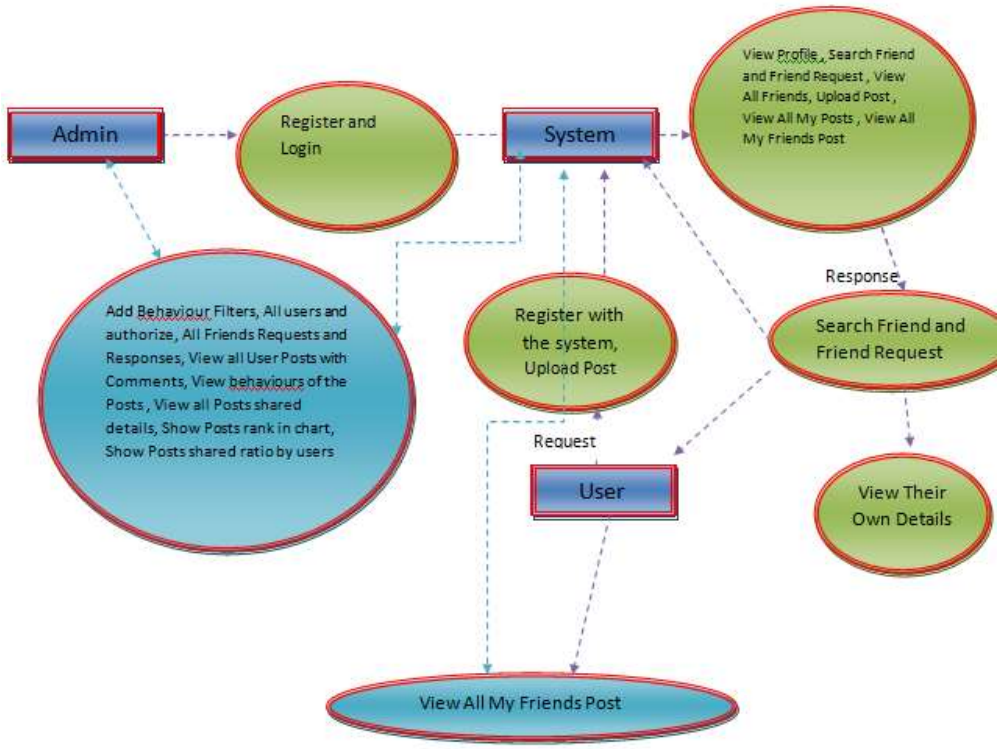


International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

B. **System Flowchart**

The process begins with user login → file selection and client-side encryption → upload to server → generation of secure shareable link → recipient accesses link → decryption in browser → optional feedback or versioning.

➢ **Data Flow Diagram :**



C. Modules Overview

- **Data Owner**

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Attackers, Upload File, View Files, Verify data(Verifiability), View and Delete Files, View All Transactions.

Cloud Service Provider

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The **Cloud** server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, View and Authorize Users, View and Authorize Owners, View Files, View All Search Transactions, View All File Transactions, View All Top Searched, View Attackers, Search Requests, View Time Delay, View Throughput.

- **User**

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and performing the following operations Register and Login, My Profile, View Files, Search Files, Search Ratio, Top K Search, Req Search Control.

- **PKG– responsible for viewing Files and Generate Key.**

Table I: Technology Stack

Component	Technology / Tool
Programming Language	JavaScript (Frontend), Java / Node.js (Backend)
Encryption	AES-256 via Web Crypto API
Web Framework	React.js / HTML5, CSS3, Bootstrap
Database	MySQL / MongoDB (for metadata only)

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Component	Technology / Tool
Backend	Node.js / Spring Boot
Cloud Storage	Compatible with AWS S3, Azure Blob, etc.
Visualization	Chart.js
OS	Platform Independent (Web Browser)

Table II: Performance / Evaluation Summary

Metric / Component	Web Cloud	Traditional Cloud Storage	Remarks
Encryption Type	Client-side (End-to-End)	Server-side	Zero-knowledge security
Data Confidentiality	High (Provider cannot access)	Medium	Stronger privacy
Cross-Platform Access	Excellent (Web-based)	Good	Browser compatibility
Sharing Security	High (Expiration + Password)	Moderate	Granular control
Performance Overhead	Low	Minimal	Acceptable for security gain
Usability	High	High	Responsive web interface

Screenshots (in the actual document) illustrate the clean interface, upload process, encryption status, and secure sharing features.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig 1:- home page

Fig2 :-cloud service home page

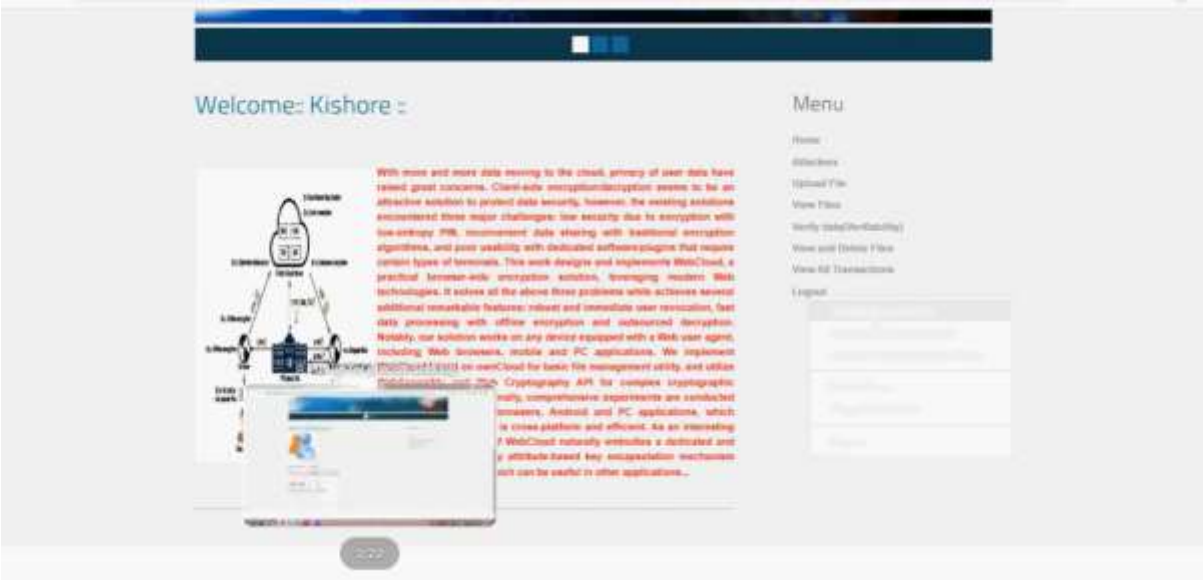


Fig :- Data owner home page

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

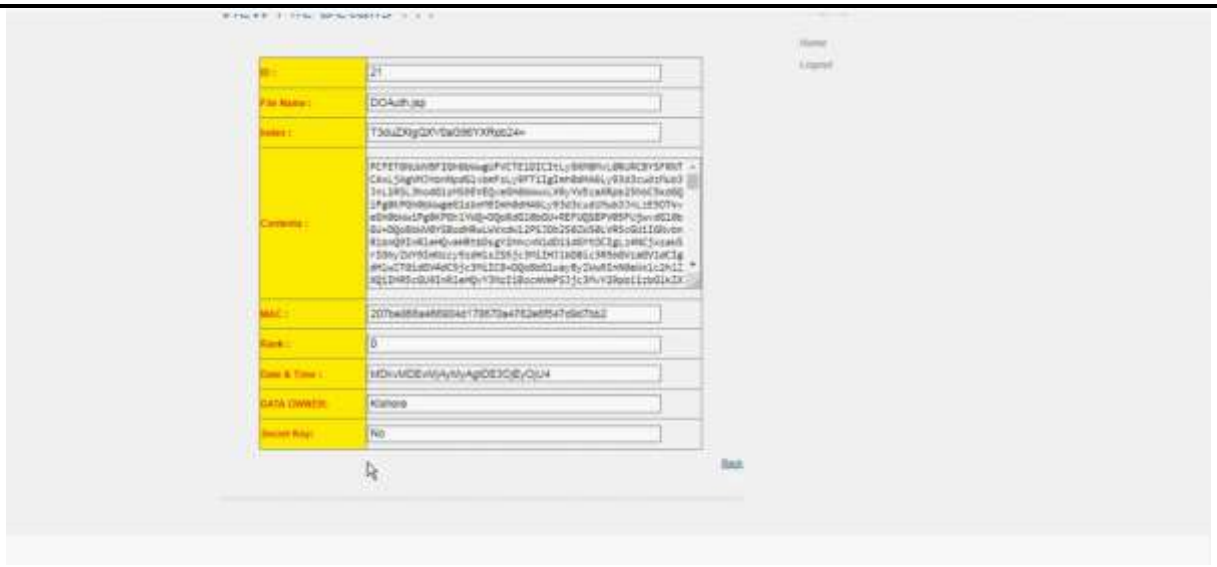


Fig 4:- Encrypt the file which is uploaded by dataowner

Fig 5 :- search the file to download the file

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Fig 6:- download the file using secret key

VI.Conclusion

This project presented Web Cloud, a secure web-based cloud storage system that enables safe data storage and sharing across platforms. By performing encryption entirely on the client side and adopting a zero-knowledge approach, the system significantly reduces privacy risks associated with traditional cloud providers.

Web Cloud offers a practical balance between strong security and user-friendly experience. Its modular design, cross-platform compatibility, and robust access controls make it suitable for both individual users and enterprise environments. The project demonstrates the effectiveness of modern web technologies in building secure cloud storage solutions and lays a foundation for future enhancements such as integration with decentralized storage or advanced attribute-based encryption.

References

1. WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms.
2. Studies on Client-Side Encryption in Cloud Storage.
3. Research on Access Control Mechanisms for Secure Data Sharing.
4. Surveys on Cloud Security Challenges and Solutions.
5. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
6. 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
7. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

8. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
9. 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.
10. 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
11. 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
12. 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.
13. 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.
14. 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
15. 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.
16. 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
17. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
18. 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.
19. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
20. 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
21. 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.
22. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
23. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.

24. 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.
25. 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
26. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
27. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
28. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
29. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
30. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
31. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
32. 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.
33. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
34. 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
35. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
36. 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.
37. 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.
38. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
39. 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
40. 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

41. 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.
42. 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.
43. 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.
44. 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).
45. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
46. 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.
47. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
48. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
49. 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
50. 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.
51. 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.
52. 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).
53. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
54. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
55. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

56. 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.
57. 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.