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

RISK ASSESSMENT IN SOCIAL NETWORKS BASED ON USER ANOMALOUS BEHAVIORS

BONAM RUPA LAKSHMI SAI BHAVANI
Department of MCA
SKBR PG COLLEGE, AMALAPURAM, A.P
bonamrupa9@gmail.com

Abstract

Online Social Networks (OSNs) have become integral to modern communication, enabling users to connect, share information, and engage globally. However, the open nature of these platforms exposes them to various security and privacy risks from users exhibiting anomalous behaviors, such as fake accounts, compromised profiles, spam campaigns, coordinated misinformation, and cyberbullying.

Risk Assessment in Social Networks Based on User Anomalous Behaviors is a machine learning-driven framework designed to detect and quantify risks associated with deviant user activities. The system analyzes user behavioral patterns (posting frequency, interaction graphs, content semantics, and temporal activity) to identify deviations from normal behavior. It employs unsupervised anomaly detection techniques, including clustering of similar users, behavioral modeling, and metrics like deviation scores to assign risk levels to individual users or groups.

By grouping users with similar profiles (based on demographics, activity levels, and network structure) and building group-specific normal behavior models, the framework achieves higher accuracy than global models. Experiments on real-world datasets (e.g., Facebook-like graphs) demonstrate effective detection of diverse anomalous behaviors such as Sybil attacks, click-spam, and collusion networks while maintaining low false positives. This approach enhances platform security, reduces malicious activity, and supports proactive risk mitigation for OSN providers and users.

Keywords: Social Network Security, Anomaly Detection, User Behavior Analysis, Risk Assessment, Unsupervised Machine Learning, Graph-Based Anomaly Detection, Sybil Attack Detection.

I.Introduction

Online Social Networks (OSNs) such as Facebook, Twitter (X), Instagram, and LinkedIn have transformed how individuals interact, share information, and build communities. With billions of active users, these platforms generate vast amounts of behavioral data daily. While they offer significant societal benefits, they also introduce serious risks including identity theft, misinformation spread, cyberbullying, spam, and coordinated attacks by malicious actors.

Anomalous user behaviors — actions that significantly deviate from typical patterns — often signal potential threats. Examples include sudden spikes in posting activity, unusual friend

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

request patterns, repetitive content sharing, or interactions inconsistent with a user's historical profile. Traditional rule-based or supervised detection methods struggle with evolving attack strategies and require labeled data, which is often scarce or outdated.

This project presents a comprehensive risk assessment framework that quantifies the risk level of users based on the degree of divergence from normal behavior. The core idea is that the greater the deviation, the higher the associated risk. The system operates in two phases: (1) grouping similar users to create personalized behavioral baselines, and (2) measuring divergence using statistical and machine learning models.

The framework supports real-time or near-real-time monitoring and can be integrated into OSN platforms for automated alerts, account flagging, or enhanced verification. It addresses limitations of existing methods by being unsupervised and adaptive to group-level variations in user behavior.

II. Literature Survey

Research on anomaly detection in social networks has evolved from structural graph analysis to behavioral and hybrid approaches.

- Laleh et al. (2016) proposed a risk assessment model based on user anomalous behaviors in OSNs. They grouped similar users and built behavioral models per group, showing improved performance over global models on Facebook datasets.
- Viswanath et al. (2014) introduced unsupervised PCA-based anomaly detection for detecting fake likes, Sybil accounts, and compromised users in Facebook, achieving effective identification without prior attack knowledge.
- Savage et al. (2016) surveyed anomaly detection techniques in OSNs, classifying them into static/dynamic and labeled/unlabeled categories, covering graph-based, content-based, and temporal methods.
- Yu et al. (2016) reviewed social media anomaly detection, highlighting point anomalies (individual user behavior) and group anomalies (coordinated activities), with techniques ranging from scan statistics to tensor decomposition.
- Xing et al. (2024) provided a recent survey categorizing methods into user behavioral features, network topological structure, and collaborative fusion approaches, emphasizing challenges in large-scale dynamic networks.
- Additional works explore graph neural networks, isolation forests, autoencoders, and UEBA (User and Entity Behavior Analytics) for risk scoring in social and enterprise environments.

These studies underscore the shift toward unsupervised and hybrid methods capable of handling diverse, evolving anomalous behaviors in social networks.

III. Existing System & Proposed System

A. Existing System

Current OSN security mechanisms primarily rely on:

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

- Rule-based filters for spam and abusive content.
- Supervised machine learning trained on known attack patterns.
- Manual reporting and behavioral thresholds.

Disadvantages of Existing Systems:

1. High dependency on labeled data.
2. Poor detection of subtle or group-level anomalies.
3. Global models ignore user diversity.
4. High false positive rates.
5. Limited risk quantification.
6. Scalability issues.

B. Proposed System

The proposed system introduces a two-phase risk assessment framework:

Phase 1: User Grouping — Cluster users based on demographics, activity levels, and network features.
Phase 2: Behavioral Modeling & Risk Scoring — Build normal profiles and compute deviation-based risk scores.

The system integrates behavioral and graph-based features, assigning continuous risk scores and enabling automated interventions.

Supports real-time streaming data analysis using incremental learning.

Incorporates temporal anomaly detection to track behavior evolution.

Enables risk categorization (Low / Medium / High) for better decision-making.

Can be extended to cross-platform analysis (e.g., linking behavior across multiple social media accounts).

Provides explainable risk scores for transparency and trust.

Advantages of the Proposed System:

1. Unsupervised detection.
2. Improved accuracy via group-aware modeling.
3. Continuous risk scoring.
4. Scalable with modern ML techniques.
5. Adaptive to evolving behaviors.
6. Detects diverse anomalies.
7. Privacy-aware design.

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

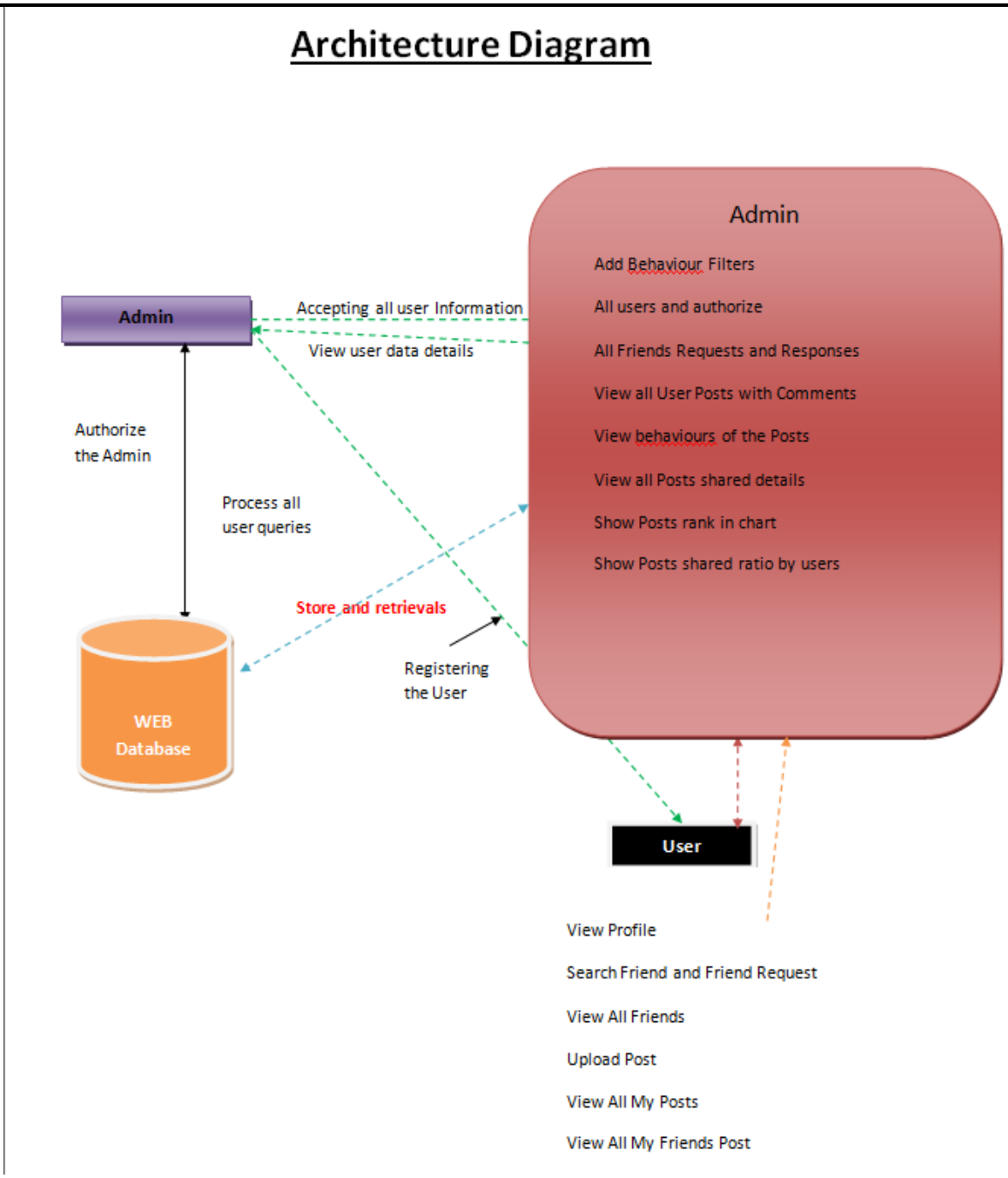
IV. System Design & Architecture

A. System Architecture

The architecture includes:

- Data Collection Layer
- Feature Extraction Layer
- User Grouping Module
- Anomaly Detection & Risk Engine
- Risk Scoring & Alert Module
- Visualization & Feedback Module

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

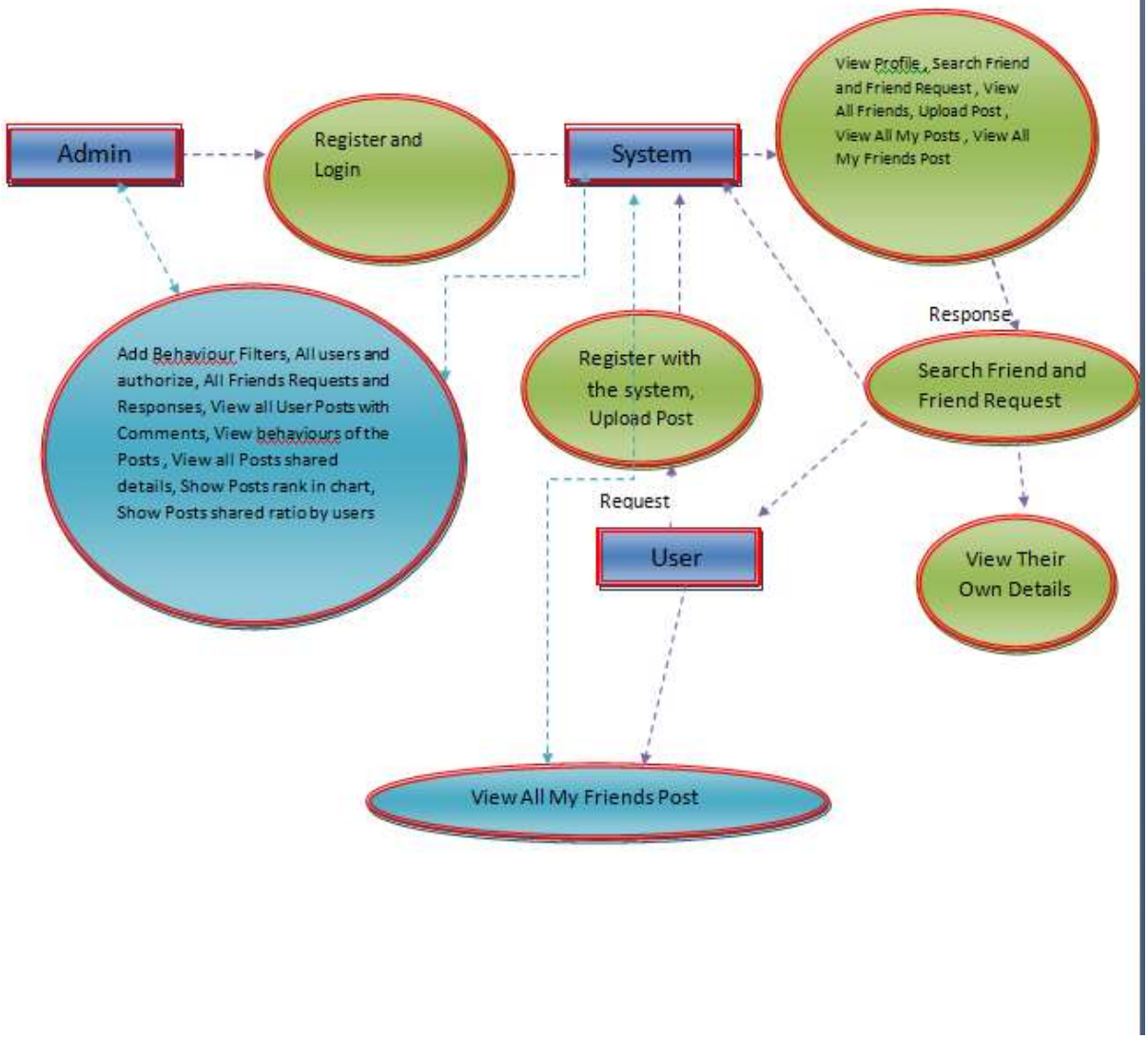


B.System Flow:

Data flow: Raw activity → Feature extraction → Grouping → Modeling → Risk scoring → Alerts.

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

➢ Data Flow Diagram :



B. Modules Overview

- **Admin**

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as Add Behaviour Filters, All users and authorize, All Friends Requests and Responses, View all User Posts with Comments, View behaviours of the Posts , View all Posts shared details, Show Posts rank in chart, Show Posts shared ratio by users

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

Friend Request & Response

In this module, the admin can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting.

- **User**

In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Verify finger print and Login Once Login is successful user can perform some operations like View Profile , Search Friend and Friend Request , View All Friends, Upload Post , View All My Posts , View All My Friends Post

Searching Users to make friends

In this module, the user searches for users in Same Network and in the Networks and sends friend requests to them. The user can search for users in other Networks to make friends only if they have permission.

Table I: Technology Stack

Component	Technology / Tool
Programming Language	Python 3.10+
ML / Anomaly Detection	Scikit-learn, TensorFlow / PyTorch
Graph Processing	NetworkX, Graph Neural Networks
Web Framework	Flask / Streamlit
Database	MySQL / PostgreSQL
Visualization	Matplotlib, Seaborn, Plotly
Deployment	Docker, Cloud platforms

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

Table II: Performance / Evaluation Summary

Metric	Proposed System	Traditional Models	Remarks
Detection Accuracy (F1)	85–95%	60–80%	Group-aware modeling
False Positive Rate	Low	Higher	Personalized baselines
Risk Quantification	Continuous	Binary	Better prioritization
Scalability	High	Limited	Handles large graphs
Adaptability to New Attacks	Excellent	Poor	Unsupervised approach

Fig 1:-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 2:- Admin Home page

Fig 3:- Add Behaviour Keywords

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:- Result of Attacking Behivour

Fig 5:-Software attacks behaviour

VI.Conclusion

This project presented a robust risk assessment framework for detecting anomalous user

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

behaviors in social networks. By combining user grouping with deviation-based modeling, the system provides accurate and scalable risk analysis without relying on labeled data.

The framework enhances platform security, enables proactive detection, and supports administrators in mitigating risks effectively. Future enhancements include integration with graph neural networks, real-time analytics, and privacy-preserving techniques.

The system bridges the gap between **security** and usability in OSNs.
It provides a proactive defense mechanism rather than reactive detection. .The framework can be generalized to other domains such as banking fraud detection and insider threat detection.

Future Enhancements:

- Multimodal data integration
- Real-time streaming analysis
- Explainable AI models
- Federated learning
- Cross-platform evaluation

This work contributes to safer and more secure online social environments.

References

1. N. Laleh et al., “Risk Assessment in Social Networks Based on User Anomalous
2. Behaviors,” IEEE Trans. Dependable and Secure Computing, 2018.
3. B. Viswanath et al., “Towards Detecting Anomalous User Behavior in Online Social Networks,” USENIX Security, 2014.
4. D. Savage et al., “Anomaly detection in online social networks,” Social Network Analysis and Mining, 2016.
5. R. Yu et al., “A Survey on Social Media Anomaly Detection,” SIGKDD Explorations, 2016.
6. L. Xing et al., “A survey on social network’s anomalous behavior detection,” Complex & Intelligent Systems, 2024.
7. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
8. 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
9. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
10. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
11. 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.

12. 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
13. 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
14. 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.
15. 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.
16. 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
17. 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.
18. 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
19. Maturi, S. Y. (2025). Vulnerabilities in the 802.11 Wireless Client Selection Mechanis.
20. 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.
21. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
22. 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
23. 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.
24. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
25. Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
26. 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.

27. 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
28. Maturi, S. Y. Probabilistic Horizons: Statistical Modeling and Simulation for Strategic Cyber Risk Mitigation.
29. Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).
30. Kotte, G. (2025). Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283668
31. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
32. Kotte, G. (2025). Revolutionizing Stock Market Trading with Artificial Intelligence. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283647
33. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
34. 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.
35. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).
36. 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
37. Manoharan, D. (2026). AI-Driven Anomaly Detection Models for Preventing Claims Denials and Revenue Leakage in Healthcare. Available at SSRN 6385759.
38. 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.
39. 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.
40. Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
41. 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
42. 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

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

43. 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.
44. 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.
45. 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.
46. 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).
47. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
48. 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.
49. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
50. Mudusu, S. K. (2025, December 22). Cognitive data architecture: Designing self-optimizing frameworks for scalable AI systems. CIO (Foundry Expert Contributor Network).
51. 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
52. 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.
53. 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.
54. 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).
55. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
56. DEVARASETTY, N. (2023). SCALABLE DATA ENGINEERING APPROACHES FOR AI-DRIVEN INDUSTRIAL IOT APPLICATIONS. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND MANAGEMENT, 11(06), 954-968.
57. Mudusu, S. K. (2025, April 20). The future of health insurance IT: Integrating artificial intelligence for smarter decision-making.
58. 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.

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

59. 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.