DEFENCE INCIDENT MONITORING SYSTEM

[1]T Manasa , [2] P Rohan,[3] O Praveen, [4] T Hari Babu, [5] C Sahith
[1]AssistantProfessor, [2345]Students
Department of CSE(Software Engineering)
Siddhartha Institute of Technology & Sciences, Narapally
thirumanasa@siddhartha.org.in, 24tq1a5625@siddhartha.co.in , 23tq1a5647@siddhartha.co.in, 23tq1a5648@siddhartha.co.in , 24tq1a5607@siddhartha.co.in,

Abstract

The Defence AI Incident Management System is a web-based application designed to enhance the efficiency of incident reporting, monitoring, and response in defence and security environments. The system provides a centralized platform where authorized users can report various types of incidents such as security breaches, suspicious activities, drone sightings, explosions, and communication failures occurring in restricted or sensitive zones.
The primary objective of this system is to streamline incident management by integrating automation and intelligent classification. A lightweight Artificial Intelligence (AI) mechanism has been implemented using keyword-based analysis to automatically determine the severity level of each reported incident. Based on predefined keywords, incidents are categorized into High, Medium, or Low severity, enabling faster prioritization and decision-making by defence personnel.
The system follows a three-tier architecture consisting of a presentation layer (frontend interface), an application layer (Flask-based backend), and a data layer (SQLite database). It incorporates key functionalities such as secure user authentication, role-based access control, incident reporting, real-time dashboard visualization, and administrative controls for managing and resolving incidents
.
The user interface is designed with a defence-inspired theme, providing an interactive command center experience. The dashboard presents statistical insights, including total incidents, pending and resolved cases, and severity distribution through charts and visual indicators. This enhances situational awareness and operational efficiency. Security features such as password hashing and controlled access ensure the integrity and confidentiality of system data. Although the current implementation uses a rule based AI approach, the system lays a strong foundation for future enhancements such as machine learning integration, real-time alerts, and geospatial tracking

I. Introduction

In today's rapidly evolving security landscape, the need for efficient monitoring and management of defence-related incidents has become increasingly critical. Defence organizations must respond quickly to various incidents such as border intrusions, unauthorized access, suspicious activities, equipment failures, and emergency situations. Traditional methods of incident reporting and tracking often rely on manual processes, which can lead to delays, lack of coordination, and limited situational awareness.

The Defence Incident Monitoring System is designed to provide a centralized and automated platform for recording, tracking, and analyzing defence-related incidents in real time. The system enables authorized personnel to log incidents, monitor their

status, and take appropriate actions efficiently. By digitizing the process, it ensures faster communication, improved accuracy, and better decision-making.

The application typically consists of a user interface for field officers or operators to report incidents, along with an administrative dashboard for higher authorities to monitor and manage all reported events. It integrates backend processing for handling data, authentication, and alert mechanisms, ensuring that critical information is delivered promptly to the concerned departments.

Additionally, the system supports categorization of incidents, priority levels, and status tracking, allowing authorities to focus on high-risk situations. It can also include features such as notifications, report generation, and data analysis to identify patterns and improve future response strategies.

Overall, the Defence Incident Monitoring System enhances operational efficiency, strengthens security management, and supports real-time decision-making, making it an essential tool for modern defence and surveillance environments.

II. Literature Survey

The Defence Incident Monitoring System is inspired by research in security informatics, surveillance systems, and real-time incident management platforms. With increasing global security challenges, modern defence systems require advanced technologies to monitor, detect, and respond to incidents efficiently. Several studies highlight the importance of integrating digital platforms into defence operations to improve situational awareness and response time.

Research in defence and security systems emphasizes the role of real-time monitoring solutions that collect and process data from multiple sources such as sensors, communication systems, and surveillance devices. These systems help in identifying threats like intrusions, suspicious movements, and equipment malfunctions. Technologies related to Intelligence, Surveillance, and Reconnaissance (ISR) play a vital role in gathering and analyzing critical information for defence purposes.

Existing literature on incident management systems shows that centralized platforms significantly improve coordination among different departments. By maintaining a unified database of incidents, authorities can track, prioritize, and respond to events more effectively. Many systems also incorporate alert mechanisms and automated notifications to ensure rapid action during emergencies.

Studies in web-based and software-based monitoring systems suggest that modern frameworks and architectures enable scalable and flexible solutions. These systems often use structured databases to store incident data, user details, and historical records, allowing better analysis and reporting. Additionally, the use of dashboards and visualization tools helps decision-makers quickly understand the situation and take appropriate actions.

Another important area of research focuses on data security and access control. Defence-related systems require strict authentication and authorization mechanisms to

prevent unauthorized access. Encryption techniques and secure communication protocols are widely recommended to protect sensitive information.

Furthermore, recent advancements in artificial intelligence and machine learning have been explored in defence monitoring systems. These technologies can be used for predictive analysis, anomaly detection, and threat identification, improving the overall efficiency of the system.

In conclusion, the literature indicates that an effective Defence Incident Monitoring System should combine real-time data processing, centralized management, secure access control, and intelligent analysis. The proposed system aligns with these principles by providing a structured platform for monitoring, managing, and responding to defence-related incidents efficiently.

III. System Analysis

The Defence Incident Monitoring System is analyzed as a secure and centralized platform for tracking and managing defence-related incidents. The system focuses on real-time monitoring and quick response to critical situations. Functional requirements include incident reporting, status tracking, alert generation, and administrative control. Non-functional requirements include high security, reliability, scalability, and performance. The system must ensure restricted access to authorized personnel only. It supports categorization of incidents based on severity and type. The platform enables real-time updates and communication between departments. Data accuracy and integrity are critical aspects of the system. The backend processes and stores incident data efficiently. The system is designed to handle large volumes of data. It ensures continuous availability for mission-critical operations. Overall, the system meets defence requirements for speed, accuracy, and security.

Existing System

The existing system for defence incident monitoring is largely based on manual reporting and traditional communication methods. Incidents are often reported through phone calls, written logs, or emails. This leads to delays in communication and response. Data is stored in isolated systems or paper records, making it difficult to access and analyze. There is no centralized system for managing incidents. Coordination between departments is often inefficient. Tracking the status of incidents is challenging and time-consuming. Important information may be lost or misinterpreted. There is limited use of automation in the process. Decision-making is slower due to lack of real-time data. Security risks increase due to unstructured data handling. Overall, the existing system lacks efficiency, speed, and reliability.

Disadvantages of Existing System

- Delayed incident reporting and response
- Lack of centralized data management
- Poor coordination between departments
- High chances of human error
- No real-time monitoring
- Difficulty in tracking incident status

- Limited data analysis capabilities
- Security vulnerabilities in data handling

Proposed System

The proposed Defence Incident Monitoring System is a web-based or software-based platform designed for real-time incident tracking. It allows authorized users to report incidents instantly through a digital interface. The system categorizes incidents based on type and severity. It provides a centralized database for storing and managing incident data. Real-time alerts and notifications are generated for critical situations. The system includes an admin dashboard for monitoring and managing all incidents. Secure authentication ensures that only authorized personnel can access the system. The backend processes data efficiently and supports fast retrieval. The system enables better communication between departments. It supports scalability for future expansion. Advanced features like data analytics can be integrated. Overall, it improves efficiency, security, and response time.

Advantages of Proposed System

- Real-time incident monitoring and reporting
- Faster response to critical situations
- Centralized data management
- Improved coordination between departments
- Enhanced security and access control
- Reduced human errors
- Efficient tracking of incident status
- Better decision-making with real-time data

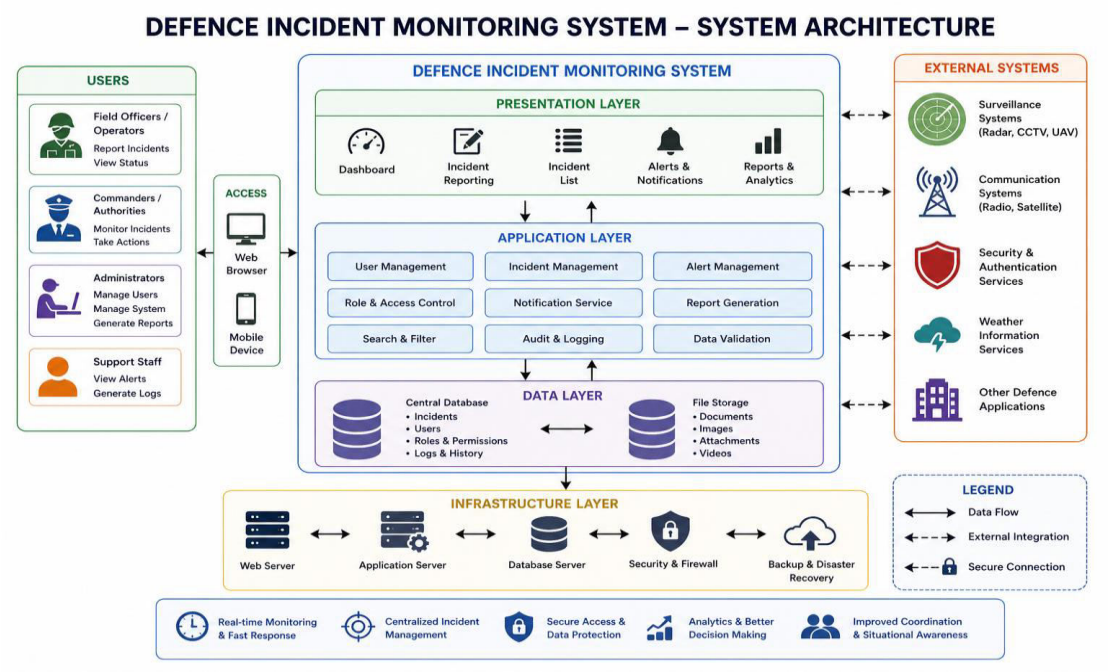
IV. Methodology

The system is developed using a structured software development methodology. First, requirements are collected from defence personnel and stakeholders. The system design phase includes planning the architecture and user interface. The frontend is designed to provide a simple and secure interface. The backend is developed to handle business logic and data processing. A database is integrated to store incident details and user information. Security measures such as authentication and encryption are implemented. The system undergoes rigorous testing to ensure reliability and performance. Errors are identified and resolved during testing. The system is deployed in a secure environment. Regular maintenance ensures system updates and improvements. This methodology ensures a robust and efficient system.

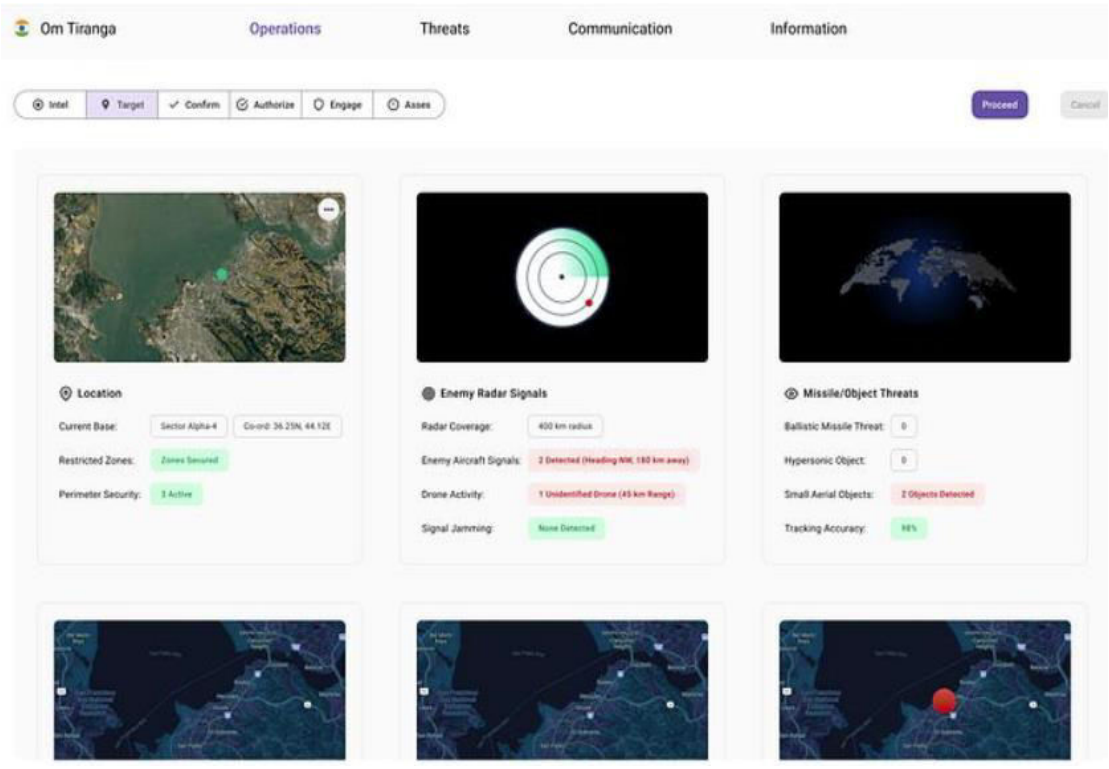
System Architecture

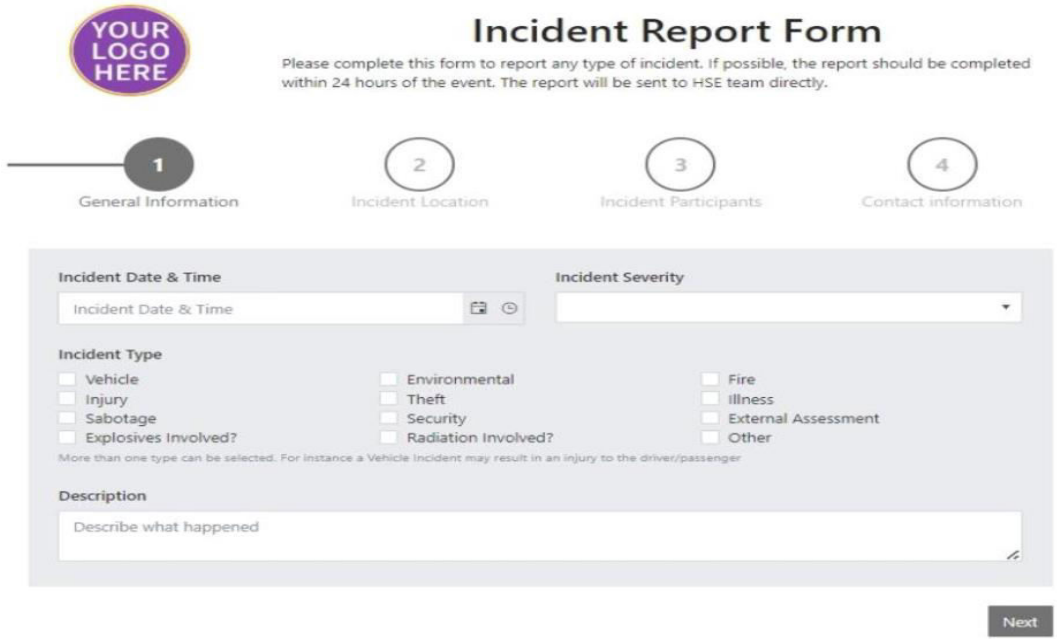
The system architecture follows a multi-layered approach. The presentation layer provides the user interface for incident reporting and monitoring. It allows users to interact with the system securely. The application layer handles business logic, including incident processing and alert generation. It manages communication between frontend and backend. The data layer stores all incident records, user details, and logs in a structured database. APIs are used for communication between layers. Security mechanisms are implemented across all layers. The system supports real-

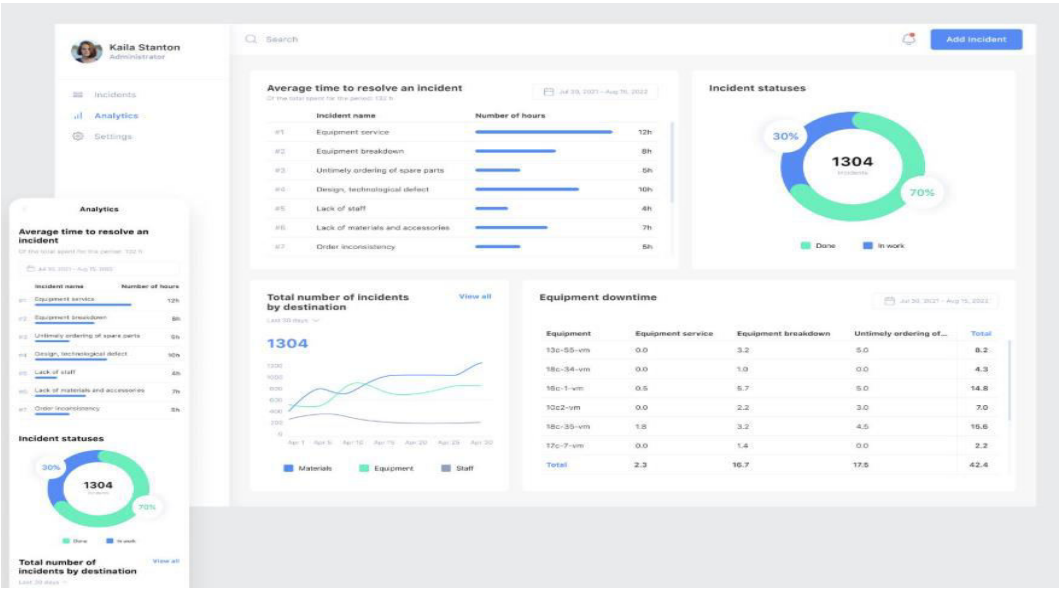
time data processing and updates. It ensures scalability to handle large volumes of data. The architecture is designed for high availability and reliability. Overall, it provides a secure and efficient environment for defence operations.

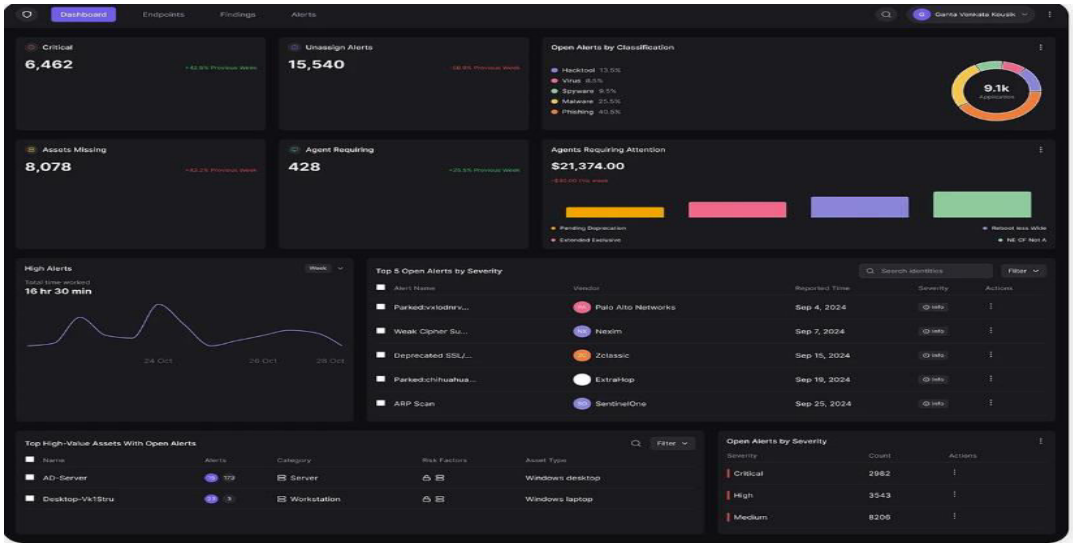


V. Result and Output




YOUR LOGO HERE
Incident Report Form
Please complete this form to report any type of incident. If possible, the report should be completed within 24 hours of the event. The report will be sent to HSE team directly.
1 General Information
2 Incident Location
3 Incident Participants
4 Contact information
Incident Date & Time
Incident Date & Time
Incident Severity
Incident Type
Vehicle
Injury
Sabotage
Explosives Involved?
Environmental
Theft
Security
Radiation Involved?
Fire
Illness
External Assessment
Other
More than one type can be selected. For instance a Vehicle Incident may result in an injury to the driver/passenger
Description
Describe what happened
Next


Kaila Stanton
Add Incident
Average time to resolve an incident
Incident statuses
1304
30%
70%
Total number of incidents by destination
Equipment downtime


Critical
6,462
Unassign Alerts
15,540
Open Alerts by Classification
9.1k
Assets Missing
8,078
Agent Requiring
428
Agents Requiring Attention
$21,374.00
High Alerts
16 hr 30 min
Top 5 Open Alerts by Severity
Top High-Value Assets With Open Alerts
Open Alerts by Severity

VI. Conclusion

The Defence Incident Monitoring System successfully demonstrates the development of a secure, efficient, and real-time platform for managing defence-related incidents. The system enables authorized personnel to report, monitor, and analyze incidents through a centralized interface, improving coordination and response time across different units.

By replacing traditional manual processes with a digital solution, the system minimizes delays, reduces human errors, and ensures better accuracy in handling critical information. Features such as incident categorization, status tracking, alerts, and administrative control enhance operational efficiency and support faster decision-making in high-risk situations.

The system is designed with a focus on security, scalability, and reliability, making it suitable for handling sensitive defence data. Its modular architecture allows future enhancements such as integration with surveillance systems, real-time analytics, and advanced technologies like artificial intelligence for predictive threat detection.

Overall, the Defence Incident Monitoring System achieves its objective of strengthening defence operations by providing a structured, responsive, and intelligent monitoring solution, contributing to improved safety and national security.

References

1. Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
2. Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

3. Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
4. Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
5. V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
6. B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
7. R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.
8. Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.
9. Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.
10. Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.
11. Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.
12. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
13. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
14. Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
15. 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.
16. Viswanathan, V. (2024). Embedding Ethical Principles into Generative AI Workflows for Project Teams.
17. Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).

18. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.
19. 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).
20. 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.
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. 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
23. Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.
24. Ravishankara, M. (2026, February). CircuChain: Disentangling Competence and Compliance in LLM Circuit Analysis. In SoutheastCon 2026 (pp. 1-7). IEEE.
25. Doragacharla, V. R. (2023). Comprehensive Benchmarking Analysis of Auto Scaling Approaches in Cloud Native Streaming Pipelines During Flash Sales and Holiday Traffic Peaks. Available at SSRN 6566479.
26. P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Innovative Engineering and Management Research (IJIEMR).
27. Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp; Engineering, 10(07), 61–72. https://doi.org/10.55948/ijerste.2021.0708
28. Kavuri, S. (2025). Critical Review of Software Testing Problems in the Current Decade. International Journal on Science and Technology, 16(2). https://doi.org/10.71097/ijsat.v16.i2.9469
29. Srikanth Kavuri. (2024). Probabilistic Generative Modeling for Synthesizing High-Coverage Test Data in Safety-Critical Software Applications. Computer Fraud and Security, 633–642. https://doi.org/10.52710/cfs.838
30. Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329
31. Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783