INTERNATIONAL JOURNAL OF PHARMACY WITH MEDICAL SCIENCES
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3068-2738
Vol.6, No. 2(1)(2026)
www.ijpams.com

UPI FRAUD DETECTION SYSTEM

Ms. Debasmita Parida
Department of Computer Science and Engineering (Artificial Intelligence)
GIFT Autonomous, Bhubaneswar, Odisha, India

Ms. Shristi Mohanty
Department of Computer Science and Engineering GIFT Autonomous, Bhubaneswar, Odisha, India

Guide: Asst. Prof. Pranab Kumar Mohanta
Department of Computer Science and Engineering
GIFT Autonomous, Bhubaneswar, Odisha, India

ABSTRACT

Now a days Digital transactions are rapidly increasing as it results in increasing online payment frauds too. In fact, according to the Reserve Bank of India, comparing March 2022 to March 2019, digital payments have risen in volume and value by 216% and 10%, respectively. People are starting to go all-in with digital transactions, but one can't deny the security issues that loom, and know-how when it comes to online payments. Few years ago, we could have barely seen the online payment, but today UPI payment QR code installed at doorstep. This invited the hoaxers and attackers to develop fraudulent transactions and fool people for some amount of money. Fortunately, the online transactions are monitored and hence could be analysed using the latest tools. In this system, an attempt is made to develop a machine learning model to identify fraudulent transactions in a transaction's dataset. This study considers the task of applying artificial intelligence to recognize bank fraud. In recent years, due to the COVID-19 pandemic, bank fraud has become even more common due to the massive transition of many operations to online platforms and the creation of many charitable funds that criminals can use to deceive users. The study's scientific novelty is the development of machine learning models for identifying fraudulent banking transactions and techniques for preprocessing bank data for further comparison and selection of the best results. This paper also details various methods for improving detection accuracy, i.e., handling highly imbalanced datasets, feature transformation, and feature engineering. The recognition of banking fraud using artificial intelligence algorithms is a topical issue in our digital society.

Keywords: Transaction, Payment, UPI, Attackers, Fraudulent, Hoaxers, Money, Dataset, artificial intelligence; fraudulent banking operations; machine learning; recognition of fraudulent operations

1. INTRODUCTION

Mobile payment has gained significant popularity as a mainstream payment method, leading to a high volume of transactions on online trading platforms.

Traditional fraud detection approaches primarily rely on statistical and multi-dimensional analysis techniques. However, these verification based methods struggle to uncover the underlying patterns in transaction data, limiting their effectiveness. On the other hand, big data technology and machine learning algorithms offer efficient solutions for detecting transaction fraud. Machine learning, particularly when applied to large datasets, can capture important features that traditional statistical methods fail to describe. By utilizing suitable machine learning techniques, we can build models based on existing transaction data to detect network transaction fraud, thereby mitigating associated losses.

In 2018, Zhaohui Zhang proposed a reconstructed feature convolutional neural network prediction

model specifically tailored for transaction fraud detection. This model demonstrated improved stability and classification effectiveness compared to other convolutional neural network models. However, a challenge remains in achieving high detection accuracy due to imbalanced sample labels. To address this, the paper introduces two fraud detection algorithms: one based on a Fully Connected Neural Network and another utilizing XGBoost. The former algorithm integrates two neural network models with different cross-entropy loss functions, enabling a quick and convenient design process for the combined model. The latter algorithm leverages Hyperopt to optimize the XGBoost classifier, resulting in a fraud detection model with superior performance by selecting the best parameters. These two algorithms serve different application scenarios.

2. OBJECTIVES OF THE PROJECT

The major objectives of the UPI Fraud Detection System are:

1. To develop a secure and intelligent system for detecting fraudulent UPI transactions in real time.
2. To analyze transaction patterns and identify suspicious activities using machine learning techniques
3. To minimize financial losses by preventing unauthorized and fraudulent transactions.
4. To improve the accuracy and efficiency of fraud detection compared to traditional rule-based methods.
5. To classify transactions as legitimate or fraudulent using predictive models and data analysis
6. To enhance the security and reliability of digital payment systems for users and financial institutions
7. To detect unusual transaction behaviors such as multiple rapid transfers, abnormal transaction amounts, and location mismatches.
8. To reduce false fraud alerts and ensure smooth transaction experiences for genuine users.
9. To create a scalable and automated fraud monitoring system capable of handling large transaction datasets
10. To contribute toward safer digital banking and promote trust in UPI-based online payment platforms.

3. LITERATURE SURVEY

Different Supervised machine learning algorithms like Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and SVM are used to detect. Although real-time datasets help identify fraudulent transactions, there are remaining challenges when dealing with imbalanced data. The future efforts will concentrate on addressing the problem mentioned earlier . The algorithm of the random forest itself should be improved . Multiple Supervised and Semi-Supervised machine learning techniques are used for fraud detection, but we aim is to overcome three main challenges with card frauds related dataset.

1. Strong class imbalance.

2.The inclusion of labelled and unlabelled samples, and

3.To increase the ability to process many transactions.

UPI offers real-time money transfer services with convenience, speed, and accessibility. However, the increasing dependence on digital transactions has also led to a substantial rise in cyber frauds such as phishing, QR-code scams, fake payment requests, identity theft, social engineering attacks, and unauthorized transactions. Researchers have therefore focused on developing intelligent fraud detection systems using Machine Learning (ML), Deep Learning (DL), anomaly detection, and behavioral analytics to improve transaction security.

UPI fraud detection has become an important research area due to the rapid growth of digital

payment systems in India. Existing studies demonstrate that machine learning and deep learning algorithms can effectively identify fraudulent transaction patterns. Among traditional algorithms, Random Forest and Gradient Boosting provide strong classification performance, while deep learning frameworks improve detection of sequential and hidden fraud behaviors.

4. EXISTING SYSTEM

The existing UPI fraud detection system primarily focuses on securing digital transactions through authentication mechanisms, rule-based monitoring, transaction analysis, and machine learning techniques. Most UPI applications such as PhonePe, Google Pay, and Paytm implement two-factor authentication methods including mobile verification, OTP authentication, device binding, biometric verification, and UPI PIN validation to ensure secure transactions. The current fraud detection framework monitors transaction attributes such as transaction amount, location, device information, transaction frequency, merchant details, and beneficiary history to identify suspicious activities. Most existing systems use predefined rule-based mechanisms where transactions are flagged if they exceed a certain threshold, originate from unknown devices, involve repeated failed login attempts, or are associated with blacklisted accounts. These systems can temporarily block transactions, send alerts, or request additional verification when suspicious behavior is detected.

In recent years, some advanced UPI fraud detection systems have integrated machine learning algorithms such as Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and XGBoost to improve fraud detection accuracy. These models analyze historical transaction data and classify transactions as legitimate or fraudulent based on learned patterns. Real-time alert systems using SMS, email, and push notifications are also widely implemented to warn users about suspicious payment requests, fake collect requests, and unauthorized login attempts.

Additionally, financial institutions maintain blacklists of fraudulent accounts, suspicious mobile numbers, IP addresses, and device fingerprints to reduce fraud risks. Organizations such as National Payments Corporation of India have also introduced AI-powered monitoring systems for identifying mule accounts and abnormal transaction behaviors.

However, the existing UPI fraud detection systems face several limitations. Most systems rely heavily on static rule-based approaches that cannot effectively detect newly evolving fraud techniques and sophisticated social engineering attacks. High false positive rates often result in legitimate transactions being incorrectly flagged as fraudulent, causing inconvenience to users. Existing systems also struggle with real-time processing due to the extremely high volume and speed of UPI transactions.

Furthermore, many systems lack advanced behavioral analytics such as typing patterns, user interaction behavior, and contextual transaction analysis, which reduces their ability to detect intelligent fraud activities. Another major challenge is the imbalance between legitimate and fraudulent transaction data, which affects machine learning model performance. Therefore, researchers are now focusing on hybrid AI-based fraud detection systems that combine machine learning, deep learning, anomaly detection, and behavioral analytics to improve the accuracy, scalability, and real-time efficiency of UPI fraud detection systems.

The existing UPI fraud detection system is designed to protect digital financial transactions from unauthorized access and fraudulent activities. With the rapid growth of Unified Payments Interface (UPI) services in India, digital payment platforms have implemented multiple security measures to ensure safe and secure money transfers. Current systems mainly depend on authentication techniques, transaction monitoring, rule-based detection mechanisms, and machine learning algorithms to identify suspicious activities. These systems are widely used by banks, payment gateways, and UPI applications to reduce the risk of cyber fraud and financial loss.

Most existing UPI fraud detection systems use two-factor authentication to verify the identity of users before processing transactions. This authentication process includes mobile number verification, One-Time Password (OTP) validation, UPI PIN verification, biometric authentication, and device

registration. The primary objective of these mechanisms is to prevent unauthorized users from accessing bank accounts or initiating fraudulent transactions. When a user initiates a transaction, the system validates the user credentials and device information before allowing the payment to proceed. This authentication layer forms the first level of protection in existing fraud detection systems.

Furthermore, many existing systems lack advanced behavioral analysis features such as typing behavior, touch patterns, transaction habits, and contextual user activity analysis. Without behavioral analytics, the system may fail to detect sophisticated frauds involving social engineering and identity theft.

5. PROPOSED SYSTEM

The proposed UPI fraud detection system is developed to identify and prevent fraudulent transactions in real time using machine learning, artificial intelligence, and behavioral analysis techniques.

The system includes three major modules:

1. Data Collection & Preprocessing Module
2. Fraud Detection & Behavioral Analysis Module
3. Alert & Verification Module

After preprocessing, feature engineering techniques are applied to identify important fraud-related patterns. Features such as unusual transaction amount, multiple failed login attempts, sudden location change, high-frequency transactions, and abnormal device usage are extracted for analysis. These features help the system differentiate between genuine and fraudulent transactions effectively.

The fraud detection engine continuously monitors incoming transactions in real time. Whenever a user initiates a UPI transaction, the system compares the transaction behavior with the user's historical transaction patterns.

6. SYSTEM REQUIREMENTS

6.1 Hardware Requirements

- Processor: Intel Core i3/i5 or higher
- 4 GB RAM
- 500 GB Hard Disk
- System Type: 64-bit computer
- Keyboard and Mouse
- Internet Connection

6.2 Software Requirements

- Operating System: Windows / Linux
- Programming Language: Python
- Frontend: HTML, CSS, JavaScript
- Backend: Flask / Django
- Database: MySQL
- Libraries: OpenCV, TensorFlow, NumPy

7. SYSTEM ARCHITECTURE

The UPI fraud detection system requires both hardware and software components to ensure smooth functioning, real-time fraud analysis, and secure transaction processing. The system is designed to handle large volumes of digital payment transactions efficiently while maintaining high accuracy in fraud detection. Proper system requirements are essential for implementing machine learning models, transaction monitoring mechanisms, and secure authentication processes.

The system architecture mainly consists of the following components:

1. Data Collection Module
2. Data Preprocessing Module
3. Feature Extraction Module
4. Database Module
5. Machine Learning-Based Fraud Detection Module
6. Behavioral Analysis Module

The hardware requirements of the proposed system include a computer system with a minimum Intel Core i3 or higher processor, 4 GB RAM, and at least 500 GB storage capacity. A 64-bit operating system is preferred to support machine learning libraries and data processing frameworks efficiently. A stable internet connection is also necessary because the system continuously monitors online UPI transactions and communicates with banking servers and payment gateways in real time. For large-scale implementations in banks or financial institutions,

cloud servers or high-performance systems may be required to process massive transaction datasets quickly and accurately.

The software requirements include an operating system such as Windows 10, Windows 11, or Linux. The proposed system is mainly developed using the Python programming language because of its simplicity, extensive library support, and strong machine learning capabilities. Python libraries such as Pandas, NumPy, and Matplotlib are used for data preprocessing, analysis, and visualization. Machine learning frameworks such as Scikit-learn, TensorFlow, and Keras are used to build fraud detection models and perform predictive analysis. The system may also use Flask or Django frameworks to create web-based interfaces and APIs for real-time transaction monitoring.

A database management system is required to store transaction records, fraud reports, user information, and historical data. Databases such as MySQL or MongoDB can be used for efficient data storage and retrieval. The database should support fast query processing because the fraud detection engine needs quick access to transaction history and user behavioral patterns during real-time analysis. Secure storage mechanisms are also required to protect sensitive financial information from unauthorized access.

The Candidate Module allows candidates to upload their personal details, political party information, election symbols, and campaign-related data. These details are displayed to voters during the election process. Candidates can also monitor election announcements and updates through the system interface.

The functional requirements of the system define the major operations performed by the fraud detection system. The system must support user authentication and secure login mechanisms to ensure authorized access. It should continuously monitor incoming UPI transactions and analyze them using machine learning algorithms. The system should detect suspicious transactions based on abnormal behavior, unusual transaction amounts, location changes, or multiple failed login attempts. If fraudulent activity is identified, the system should generate instant alerts and perform additional verification using OTP authentication or biometric security methods.

Fig 1: System Architecture Diagram

8. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) of the UPI fraud detection system represents the flow of transaction data between different modules of the system. It explains how data is collected, processed, analyzed, and used to detect fraudulent activities in real time. The DFD helps in understanding the overall working process and interaction between users, databases, machine learning models, and security modules.

The process begins when a user initiates a UPI transaction through a mobile banking or payment application. The transaction details such as user ID, transaction amount, receiver information, device details, IP address, location, and transaction time are sent to the data collection module. This module gathers all transaction-related information and forwards it to the preprocessing module for further analysis.

In the preprocessing stage, the raw transaction data is cleaned and organized. Duplicate records, incomplete entries, and invalid data are removed to improve data quality. The processed data is then transferred to the feature extraction module, where important fraud-related features are identified. Features such as unusual transaction amount, high transaction frequency, location changes, unknown device access, and abnormal transaction timing are extracted for fraud analysis

After feature extraction, the processed data is sent to the machine learning-based fraud detection module. In this module, machine learning algorithms compare the current transaction with historical transaction patterns stored in the database. The system analyzes whether the transaction behavior is normal or suspicious. Based on the analysis, the fraud detection engine calculates a fraud risk score for the transaction

If the calculated risk score is low, the transaction is considered genuine and is approved successfully. The transaction details are then stored in the database for future reference and behavioral analysis. However, if the system detects suspicious activity or a high fraud risk score, the transaction is forwarded to the alert and verification module.

The alert and verification module sends instant notifications to the user and system administrator regarding suspicious activity. The system may temporarily block the transaction and request additional verification such as OTP authentication, biometric verification, or account confirmation. If the user successfully verifies the transaction, it may proceed further; otherwise, the transaction is rejected and marked as fraudulent.

The database management module continuously stores transaction history, user behavioral patterns, fraud reports, and verification logs.

Thus, the Data Flow Diagram of the UPI fraud detection system clearly explains how transaction data flows through different modules, starting from transaction initiation to fraud detection, verification, alert generation, and database storage. The DFD helps in understanding the efficient working of the proposed system and ensures secure and reliable digital payment processing.

The DFD also helps identify possible vulnerabilities and improve system efficiency. By analyzing the flow of information, developers can optimize authentication processes, database communication, and election management operations.

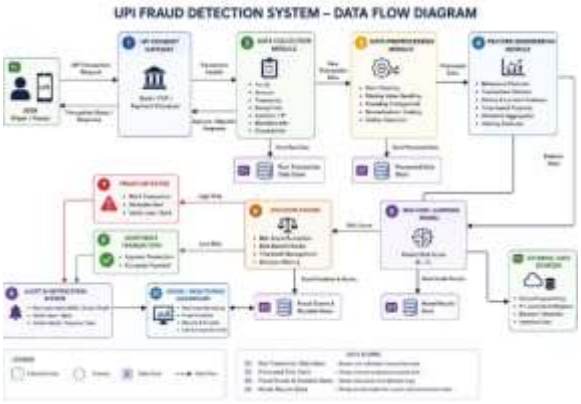

Fig 2: Data Flow Diagram

9. DATABASE DESIGN

The database design of the UPI fraud detection system is developed to store, manage, and process transaction-related information securely and efficiently. The database plays an important role in maintaining user records, transaction history, fraud reports, authentication details, and machine learning analysis results. A well-structured database helps the system perform real-time fraud detection and quick data retrieval with high accuracy.

The proposed system uses a relational database such as MySQL or a NoSQL database such as MongoDB depending on the volume and complexity of transaction data. The database is divided into multiple tables that are interconnected to ensure proper data management and reduce redundancy. Each table stores specific information related to users, transactions, fraud detection, alerts, and verification activities.

The Transaction Table stores all UPI transaction details including Transaction ID, sender ID, receiver ID, transaction amount, transaction date and time, transaction status, payment method, IP address, and device information. This table is one of the most important components because it maintains complete transaction history required for machine learning analysis and fraud monitoring.

The Fraud Detection Table stores information related to suspicious transactions identified by the machine learning model. It contains details such as Fraud ID, Transaction ID, fraud risk score, fraud type, detection time, and fraud status. This table helps

administrators analyze fraudulent activities and maintain fraud investigation records.

The Authentication Table stores user verification details such as OTP records, login attempts, biometric verification status, and authentication timestamps. This table improves system security by maintaining additional verification information for suspicious transactions.

The **Alert and Notification Table** maintains records of alerts sent to users and administrators. It stores Alert ID, Transaction ID, alert message, notification status, and alert time. This helps the system track fraud notifications and user responses effectively.

The Behavioral Analysis Table stores user behavioral patterns such as average transaction amount, preferred transaction time, frequently used devices, location history, and spending habits. This information is used by the fraud detection engine to compare current transactions with normal user behavior and identify anomalies.

The database design also includes relationships between tables using primary keys and foreign keys. For example, the Transaction Table is connected to the User Table through User ID, while the Fraud Detection Table is linked to the Transaction Table using Transaction ID.

Security is an important aspect of the database design. Sensitive information such as account details, passwords, and authentication data is encrypted to prevent unauthorized access.

Backup and recovery mechanisms are also implemented to ensure data availability and protection against system failures.

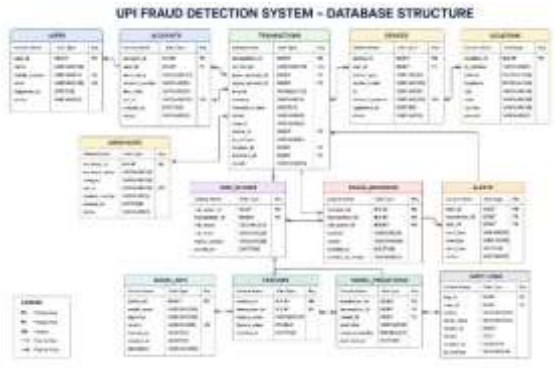

Fig 3: Database Structure

10. MODULE DESCRIPTION

10.1 Data Collection Module

This module collects transaction-related information from UPI applications, banks, and payment gateways. It gathers details such as transaction amount, sender and receiver information, device details, IP address, location, and transaction time. The collected data is stored in the database for further processing and fraud analysis.

10.2 Data Preprocessing Module

The preprocessing module cleans and organizes the collected transaction data. It removes duplicate records, handles missing values, and converts raw data into a structured format. This module improves the quality and accuracy of data before it is used for machine learning analysis.

10.3 Feature Extraction Module

This module identifies and extracts important fraud-related features from transaction data. Features such as unusual transaction amount, abnormal transaction frequency, sudden location change, and unknown device access are selected for fraud detection.

10.4 Fraud Detection Module

The fraud detection module is the core component of the system. It uses machine learning algorithms such as Random Forest, Decision Tree, Logistic Regression, and Support Vector Machine (SVM) to analyze transaction patterns and classify transactions as genuine or fraudulent. The module calculates a fraud risk score for each transaction based on user behavior and historical data.

.

Fig 4: UPI Fraud Interface

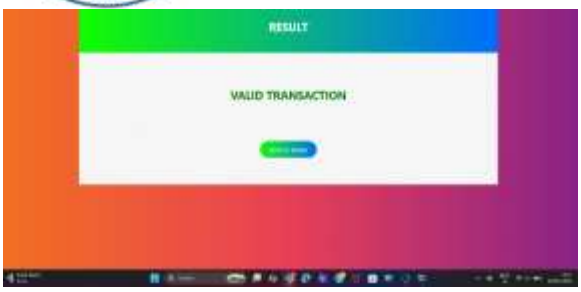

Fig 5: Dashboard

11. IMPLEMENTATION

The implementation of the UPI fraud detection system is mainly divided into three major processes: data collection and processing, fraud detection using machine learning, and alert and verification mechanisms. In the first stage, transaction data is collected from UPI applications, banks, and payment gateways. The collected data is cleaned, organized, and preprocessed to remove duplicate and incomplete records. Important fraud-related features such as transaction amount, location, device information, and transaction frequency are extracted for further analysis.

In the final stage, the alert and verification module is implemented to enhance transaction security. Whenever suspicious activity is detected, the system sends instant alerts and notifications to users and administrators. Additional security verification methods such as OTP authentication or biometric verification are performed before processing the transaction. If verification fails, the transaction is blocked or rejected. This implementation helps provide a secure, reliable, and intelligent solution for preventing fraud in UPI-based digital payment systems.

.

12. ALGORITHMS USED

12.1 Random Forest Algorithm

Random Forest is a machine learning algorithm that uses multiple decision trees to detect fraudulent transactions. It improves prediction accuracy by combining the outputs of different trees.

The process includes:

1. Data Collection and Preprocessing
2. Feature Extraction and Analysis
3. Fraud Detection Using Machine Learning
4. Alert and Verification Process

The algorithm provides fast and accurate facial detection.

12.2 Decision Tree Algorithm

Decision Tree is a supervised learning algorithm used to classify transactions as genuine or fraudulent based on transaction features. It creates a tree-like structure using conditions such as transaction amount, location, and transaction frequency.

The Decision Tree works by repeatedly splitting the dataset into smaller subsets based on the most important features.

13. RESULTS AND DISCUSSION

The proposed UPI fraud detection system was implemented and tested using machine learning algorithms to identify fraudulent and genuine transactions. The system was trained using transaction datasets containing various transaction details such as transaction amount, transaction frequency, location, device information, and user behavioral patterns.

The fraud detection model significantly reduced false transactions and improved transaction security by generating instant alerts and additional verification processes such as OTP authentication. Behavioral analysis further enhanced system performance by comparing current transaction behavior with historical user activity. This helped the system detect both known and unknown fraud patterns effectively.

14. ADVANTAGES OF THE SYSTEM

1. Detects fraudulent transactions in real time.
2. Improves security of UPI payment systems.
3. Reduces financial losses caused by fraud.
4. Provides instant alerts and notifications
5. Uses machine learning for accurate fraud detection
6. Analyzes user behavior to identify suspicious activities.

7. Reduces false fraud detection rates
8. Supports secure OTP and biometric verification
9. Handles large volumes of transaction data efficiently
10. Enhances customer trust in digital payments

15. FUTURE ENHANCEMENTS

The system can be enhanced further using advanced technologies. Future improvements include:

1. Real-time cloud-based fraud monitoring and analysis.
2. Development of mobile-based fraud alert applications
3. Automatic model updates for new fraud pattern.
4. Cloud-based transaction monitoring system.
5. Enhanced encryption and cybersecurity features
6. Automated fraud report generation and predictive analysis
7. Development of faster and more scalable real-time fraud detection systems.

These enhancements will improve system scalability, usability, and security.

16. CONCLUSION

The proposed UPI fraud detection system provides an intelligent and secure solution for identifying and preventing fraudulent digital payment transactions. By using machine learning algorithms, behavioral analysis, and real-time transaction monitoring, the system can accurately detect suspicious activities and reduce financial fraud risks.

The implementation of security features such as OTP verification, alert generation, and transaction monitoring improves the safety and reliability of UPI payment systems.

Overall, the UPI fraud detection system enhances digital payment security and provides a reliable framework for secure online transactions. It plays an important role in protecting users and financial organizations from cyber fraud in modern digital banking environments.

REFERENCES

[1] National Payments Corporation of India, “Unified Payments Interface (UPI) Guidelines and Security Framework.

[2] Reserve Bank of India, “Digital Payment Security Controls and Fraud Prevention Measures.”

[3] Machine Learning techniques for fraud detection in digital payment systems.

[4] Artificial Intelligence applications in banking and financial security systems.

[5] Studies on anomaly detection and behavioral analysis in online transaction systems.

[6] Journals related to cybersecurity, digital banking, and online payment fraud prevention.

[7] Transaction security models and authentication mechanisms for UPI-based payment applications.

[8] Research articles on real-time fraud detection systems using data mining and predictive analytics.

[9] Todupunuri, A. (2024). Explore How AI Can Be Used To Create Dynamic And Adaptive Fraud & Rules That Improve The Detection And Prevention Of Fraudulent & Activities In Digital Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5014699

[10] Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.

[11] Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.

[12] Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63

[13] Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.

[14] Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
[15] Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
[16] Poojari, R. Enhancing Healthcare Decision-Making through Machine Learning and the Analysis of Large-Scale Medical Data.
[17] Vasagam, M. (2024, August 30). Ensuring security in modern data pipelines: Practical strategies for data engineers. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2401.
[18] 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
[19] 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.
[20] Kumara, S. (2026, February). A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.
[21] 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
[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] 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
[24] Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
[25] Viswanathan, V. Generative AI for Smarter Workforce Planning and Enterprise Resource Decisions.
[26] Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
[27] Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. InfoWorld (Foundry Expert Contributor Network).
[28] 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.
[29] 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.
[30] 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.
[31] Maturi, S. Y. Cryptographic Privacy Engines: Practical Multi-Party Protocols For Confidential Database Queries.
[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] Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
[34] Manoharan, D. (2026). Advancing Healthcare EDI Interoperability Through Informatica Cloud B2B Gateway Quality Engineering. Available at SSRN 6385719.
[35] Ravishankara, M. (2026, February). PlotChain: Deterministic Checkpointed Evaluation of Multimodal LLMs on Engineering Plot Reading. In SoutheastCon 2026 (pp. 1-8). IEEE.
[36] Doragacharla, V. R. (2026). Building Real-Time Pricing Systems for Modern Retail. Available at SSRN 6451760.

[37] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465
[38] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).
[39] P. Venkata Ramana. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. Eudoxus Press Journal.
[40] Srikanth Kavuri. (2025). AI-DRIVEN TEST AUTOMATION FRAMEWORKS: ENHANCING EFFICIENCY AND ACCURACY IN SOFTWARE QUALITY ASSURANCE. International Journal of Applied Mathematics, 38(10s), 699–710. https://doi.org/10.12732/ijam.v38i10s.990
[41] Kavuri, S. (Ed.). (2024). Shift-left and shift-right testing approaches: A practical roadmap for continuous quality in agile and DevOps. Journal of Information Systems Engineering and Management, 9(4). https://doi.org/10.52783/jisem.v9i4.127
[42] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886
[43] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875
[44] 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
[45] 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
[46] Venkata Pavan Kumar Gummadi. (2025). MuleSoft Architectural Paradigms and Sustainability: A Comprehensive Technical Analysis. Journal of Computer Science and Technology Studies, 7(12), 534–540. https://doi.org/10.32996/jcsts.2025.7.12.59
[47] Gajula, S., Bondhala, S., & Margam, M. (2026). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–7. https://doi.org/10.1109/icaic67076.2026.11395835
[48] Majumder, R. Q. (2025). A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5267287
[49] Gajula, S. (2025). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD), 1–6. https://doi.org/10.1109/icoabcd67551.2025.11470865
[50] Gajula, S., & Kandula, S. T. R. (2026). Securing Financial Data in Multi-Tenant Clouds Through AI, Blockchain, and Attribute-Based Encryption. Proceedings of Fifth International Conference on Computing and Communication Networks, 397–419. https://doi.org/10.1007/978-3-032-21499-7_33