Vol.8 No.2 April 2025

Multimedia Research

Received 3 December, Revised 13 April, Accepted 26 April

# Enhancing Fraud Detection in Payment Systems with Generative AI and IoT Integration

**R. Aiyshwariya Devi**
*Department of Artificial Intelligence and Data Science*
*RMK College of Engineering and Technology, Chennai*
*aiyshwariyadevi@gmail.com, aiyshwariyaads@rmkcet.ac.in*

**Abstract:** Fraud detection in payment systems poses significant challenges to secure transactions in a digital economy. The rapid expansion of digital payment systems has amplified the challenges of detecting fraudulent activities, with conventional methods struggling to adapt to evolving fraud patterns and high transaction volumes. This study introduces an advanced framework for enhancing fraud detection in payment systems by integrating Generative AI and IoT technologies. The proposed system employs IoT-enabled payment devices to capture real-time transactional data, which is preprocessed and analyzed using Generative Adversarial Networks (GANs) to generate synthetic fraudulent patterns for model training. Additionally, discriminative AI models classify transactions based on enriched datasets, leveraging deep learning techniques for anomaly detection. This approach addresses key challenges such as data imbalance, dynamic fraud behaviors, and real-time detection requirements. Experimental validation on benchmark datasets and IoT-enabled payment devices demonstrates significant improvements in detection accuracy, reduced false positives, and scalability. The integration of IoT and AI technologies not only enhances fraud detection capabilities but also provides a secure, adaptive, and efficient solution for modern payment systems. This research highlights the transformative potential of combining Generative AI with IoT in combating financial fraud effectively. The integration of IoT (Internet of Things) and Generative AI technologies offers a promising solution to proactively detect and mitigate fraudulent activities. This paper proposes a system architecture for fraud detection leveraging IoT devices with generative AI to monitor transactions in real-time and to predict and identify fraudulent patterns. By combining data collected from IoT-enabled smart card systems with advanced AI algorithms, the proposed solution enhances accuracy and reduces false positives in fraud detection. This work provides a comprehensive framework, including real-time monitoring, anomaly detection, and adaptive learning mechanisms, to ensure a robust and scalable fraud detection system. These activities are administered so elegantly so it's almost like genuine transactions, the Sorting and Searching technique was used for oversampling. As we are integrating the IoT for double verification for the transaction to scale back the fraudulent transaction the NFC technology plays an important role in the re-authentication of the user feature selection was performed and the dataset was split into two parts, training data, and test data. The algorithms utilized in the experiment were Logistic Regression and high accuracy using Generative AI and Prompt integration techniques.

**Keywords:** IoT, Fraud detection, Logistic Regression, NFC Chip, Generative AI

***Nomenclature***

| Abbreviations | Expansion |
|---|---|
| **IoT** | Internet of Things |
| **AI** | Artificial Intelligence |
| **FLM** | Fraud Location Models |
| **SVM** | Support Vector Machines |
| **GANs** | Generative Adversarial Networks |
| **VAEs** | Variational Auto Encoders |
| **GP** | Genetic Programming |
| **NFC** | Near-Field Communication |
| **PIN** | Personal Identification Number |
| **MFA** | Multi-Factor Authentication |
| **EFTPOS** | Electronic Funds Transfer at Point of Sale |
| **PDQ** | Process DataQuickly |
| **CTLS** | contactless |
| **BJSON** | Binary JSON |
| **RBAC** | Role-Based Access Control |
| **SSL** | Secure Socket Layer |
| **PoS** | Point of Sale |

© Resbee Info Technologies Pvt Ltd
https://doi.org/10.46253/j.mr.v8i2.a1

# 1. Introduction

Fraud Detection misrepresentation can be characterized as "the unapproved utilization of a person's charge card or card data to makebuys, or to expel reserves from the cardholder's record". In today's digital economy, credit card fraud remains a critical challenge, causing financial losses and eroding consumer trust. Traditional fraud detection systems, while effective to some extent, often struggle with real-time adaptability and high false-positive rates.

The integration of Generative AI and IoT technologies presents a transformative approach to this issue. IoT-enabled devices offer real-time data acquisition and monitoring, while Generative AI models excel at identifying complex patterns and anomalies in transactional data. This paper explores how the synergy of these advanced technologies can significantly enhance credit card fraud detection, providing a scalable, efficient, and adaptive system that ensures transaction security and mitigates fraudulent activities. Credit card fraud typically begins when an individual gains unauthorized access to a credit or debit card—either by physically stealing it or by obtaining sensitive information such as the card number, expiration date, and CVV code through deceptive means. Although physical card theft still occurs, technological advancements have led to a significant rise in digital methods for capturing card data. Often, neither the cardholder, merchant, nor issuing bank is aware of the breach until the compromised information is used for fraudulent purchases.

Credit card fraud involves the unauthorized use of a payment system, where the card or its data is exploited without the cardholder's knowledge. A credit card, whether physical or virtual, acts as a tool for financial transactions. As credit card usage grows, so does the occurrence of fraudulent activity. In face-to-face transactions, a fraudster must physically steal the card. In contrast, for online or phone-based transactions, only the card details—such as the number, expiration date, and CVV—are needed, making it easier for cybercriminals to commit fraud without ever touching the physical card.

Frequently, cardholders remain unaware that their information has been compromised. Fraudulent transactions often blend in with legitimate ones, making them difficult to detect through simple rule-based systems. To identify such irregularities, data mining techniques like outlier detection are commonly used in fraud detection systems. Outliers refer to data points that differ significantly from the rest of the dataset and may indicate suspicious activity. Techniques such as neural networks, Local Outlier Factor (LOF), and Isolation Forest are effective in identifying these anomalies. Anomaly detection, or outlier detection, focuses on recognizing rare or unusual behaviors within data, which may signal fraudulent intent. Additionally, logistic regression—a statistical method using a logistic function to model binary outcomes—is also applied in fraud detection, often as part of a broader machine learning framework.

# 2. Literature Review

Different FDMs have been proposed in past years. Each model had demonstrated its great work with a one-of-a-kind dataset, however, no model fitting for all datasets. There are different models for distinguishingextortion in Credit cards:

## 2.1 Dempster–Shafer Theory and Bayesian Learning

Four segments of Dempster Shafer Theory are: manage a based channel, Dempster– Shafer snake, exchange history database, and Bayesian student.

## 2.2 Traditional Fraud Detection Techniques

**Rule-Based Systems:** Early fraud detection systems relied on predefined rules and thresholds to flag suspicious activities. For example, unusual spending patterns or transactions from unfamiliar locations would trigger alerts. While effective in certain scenarios, these systems lack adaptability to evolving fraud tactics and often result in high false-positive rates. The key limitation is the inability to learn from dynamic behavioral patterns.

**Statistical Models:** Linear regression and other statistical models were introduced to analyze transaction data for irregularities. These models improved accuracy but were computationally intensive and still limited in handling complex relationships in large datasets.

## 2.3 Machine Learning Approaches for Fraud Detection

**Supervised Learning:** Techniques like Support Vector Machines (SVM), Decision Trees, and Neural Networks have been widely used in fraud detection. These models require extensive labeled datasets to train classifiers capable of distinguishing between legitimate and fraudulent transactions.

Dependency on labeled data and inability to handle emerging fraud techniques effectively.

**Unsupervised Learning**: Clustering algorithms such as K-means and Isolation Forests identify anomalies without labeled data. These methods are useful for detecting unknown fraud patterns but struggle with distinguishing anomalies from legitimate rare behaviors.

Balancing detection accuracy with false-positive rates remains a significant issue in machine learning-based systems.

## 2.4 IoT-Based Fraud Detection

IoT devices, such as smart cards and point-of-sale terminals, have revolutionized real-time transaction monitoring. These devices capture rich transactional data, including time, location, and device-specific metrics, which can provide additional context for detecting fraudulent activities.

IoT-enabled credit card systems proposed by [Odelu V[10]] demonstrated improved detection rates by analyzing geolocation and temporal data.

Smart card designs by John Richard [2] showed how encrypted communication reduces tampering risks. The challenges identified are security vulnerabilities in IoT networks, such as susceptibility to man-in-the-middle attacks. High computational requirements for processing large volumes of IoT data in real-time.

## 2.5. Generative AI in Fraud Detection

Generative Adversarial Networks (GANs): GANs have emerged as a powerful tool for fraud detection. They model legitimate transaction patterns to identify anomalies by generating synthetic data that mimic normal behavior.

**Key Studies:** [Author Calvin [5]] demonstrated the use of GANs to detect fraudulent credit card transactions, achieving a significant reduction in false-positive rates. Anomaly detection frameworks by [Author Don James [6]] utilized Variational Auto encoders (VAEs) to capture latent representations of transactional data, effectively flagging deviations.

**Challenges Identified:** Training GANs require substantial computational resources. High dependency on high-quality datasets for effective training.

## 2.6 Hybrid Approaches Combining IoT and AI

The integration of IoT and AI technologies has been explored as a means to enhance fraud detection systems. IoT devices provide the infrastructure for real-time monitoring, while AI models analyze the incoming data for fraud detection.

[Author Elvin [7]] combined IoT-based data collection with AI-driven predictive models to achieve improved accuracy in fraud detection systems demonstrating the use of IoT data as input for deep learning models, enhancing the contextual understanding of transactional anomalies. The challenges identified are ensuring seamless communication between IoT devices and AI systems. Maintaining low latency for real-time fraud detection in large-scale deployments.

## 2.7 Gap Analysis

While significant advancements have been made in IoT and AI applications for fraud detection, a unified approach leveraging the strengths of both technologies is still underexplored.

**Current systems lack:**

- Adaptive mechanisms to handle evolving fraud techniques.
- Effective integration of IoT data streams into Generative AI models for real-time fraud detection.
- Scalable and secure architectures that can operate efficiently under large-scale deployments

**Hidden Markov Model Fraud detection:**System gets every approaching exchange andcheck the buying conduct for discovering whether the exchange is misrepresentation ornot.

**Detection of Credit Card Fraud using Fuzzy:** The fuzzy Darwinian Detection framework utilize fluffy rationale rules. The framework comprises a fluffy master framework and a GP-look calculation.

**Bayesian and Neural Networks:** Bayesian systems or conviction systems utilizemachine learning and information mining strategies for man-made brainpower.

**Fraud detection using Association Rules:** This fluffy rationale is utilized with affiliationguidelines to

conquer the challenges of the least help and certainty, enhances the execution time

# 3. Proposed Model

The first thing it will do is to activate the NFCby sending the electromagnetic signal to the chip. Then the chip which has the serial number linked with the user's card datain the bank server detects that the transactionrequest is coming from the user's card and it will fetch the database from the server.

The request is sent to the monitoring agent ofthe bank server for user verification. It searches the bank database for the user's valid information and it will update to the swiping machine.

The user is verified by the bank, this is the mainprocess of the system, after the card insertion the information will go to the bank andthe each time the user try to make payment then each time the user will receive the random system generated pin for the transaction to approve the payment.

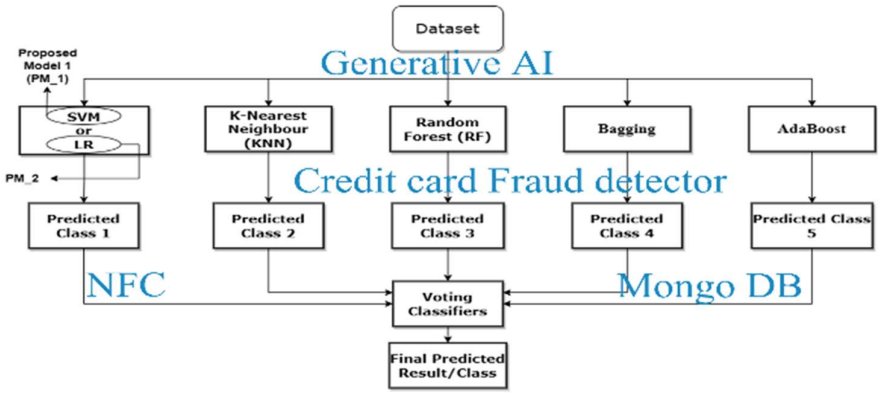


***Fig. 1.*** *Proposed Model Architecture*

## 3.1 Workflow Diagram of the Proposed Architecture

**Step 1:** A transaction is initiated via an IoT-enabled smart card.
**Step 2:** Data is transmitted to the preprocessing layer via an IoT gateway.
**Step 3:** Preprocessed data is analyzed by Generative AI and Discriminative AI subsystems.
**Step 4:** Anomaly detection results are sent to the decision layer for risk scoring and alert generation.
**Step 5:** Feedback is used to update AI models, ensuring adaptive learning.
The different layers of the proposed system are explained below

## 3.2 Data Acquisition Layer

IoT-Enabled Smart Cards: Equipped with embedded sensors and chips, smart cards capture real-time transactional data, such as:

Transaction amount, Timestamp, Geolocation, and Device ID.

The IoT gateways serve as intermediaries to securely transmit data from smart cards to the cloud or local servers using encrypted protocols like TLS.

## 3.3 Data Preprocessing Layer

During the data aggregation transaction data from multiple IoT devices into a centralized or distributed data store.

Preprocessing Pipeline includes noise filtering to remove outliers and irrelevant data. Data normalization for consistent input formats and feature engineering to extract meaningful patterns from raw data, such as transaction frequency or deviation from user norms.

## 3.4 AI Model Layer

**a) Generative AI Subsystem**

The GANs typical transaction behaviors to produce synthetic, legitimate-like data.

The discriminator detects anomalies by distinguishing between actual transactions and generated synthetic samples. VAEs Learn latent representations of transactional data to identify subtle deviations from normal patterns.

**b) Discriminative AI Subsystem**
Supervised models classify transactions into legitimate or fraudulent categories based on labeled training data.

Algorithms like Random Forests or Deep Neural Networks are used for this step.

### 3.5 Decision Layer

The risk scoring assigns a risk score to each transaction based on outputs from the AI models. High-risk transactions trigger alerts or MFA.

Low-risk transactions proceed seamlessly.

The anomaly alerts send real-time notifications to financial institutions and cardholders for suspicious activities.

### 3.6 Feedback and Learning Layer

Continuous Learning confirms or refines detected anomalies based on the use of feedback or post-transaction verification.

Updates the AI models dynamically to adapt to emerging fraud techniques.

Reinforcement learning (optional) uses confirmed cases of fraud and legitimate transactions to optimize detection algorithms.

### 3.7 Security and Communication Layer

The encryption ensures secure data transmission between IoT devices, gateways, and cloud servers.
For authentication, it uses multi-layer authentication protocols to prevent unauthorized access to the system.

### 3.8 System Integration and Scalability

Cloud Infrastructure: For large-scale deployments, cloud-based resources ensure scalability and efficient processing of vast transactional data streams.

Edge Computing (Optional): Implements local processing on IoT gateways to reduce latency for time-sensitive fraud detection tasks.

## 4. Scientific Description

### 4.1 MongoDB

MongoDB is a cross-platform, document-oriented database system categorized under NoSQL databases. It stores data in flexible, JSON-like documents, allowing for dynamic

Schemas. MongoDB supports a variety of query types, including field-specific searches, range queries, and regular expression matching. It enables the retrieval of specific fields within documents and supports the integration of user-defined JavaScript functions within queries. Additionally, queries can be configured to return a random subset of results. MongoDB also supports indexing on document fields through both primary and secondary indexes, which enhances query performance.

### 4.2 Advanced Python

Python is a high-level, general-purpose programming language known for its simplicity and readability. It provides powerful built-in data structures and supports a clear and effective approach to object-oriented programming. Python's concise syntax, dynamic typing, and interpreted nature make it particularly well-suited for scripting, rapid application development, and cross-platform deployment. These characteristics contribute to its widespread use in fields such as web development, data science, automation, and artificial intelligence.

## 4.3 Swiping Machine Simulator

***Fig. 2.*** *Swiping machine*

A swiping machine simulator replicates the functionality of a real-world payment terminal, commonly referred to as a POS terminal. These devices are used to facilitate electronic fund transfers through payment cards. The simulator typically includes components such as a secure keypad (PIN pad) for entering personal identification numbers, a display screen, and mechanisms for reading card information. It also features a network connection to communicate with payment processing systems for transaction authorization. This simulation is valuable for testing and demonstrating electronic payment processes without the need for live financial systems.

A payment terminal allows a merchant to capture required credit and debit card information and to transmit this data to the merchant services provider or bank for authorization and finally, to transfer funds to the merchant. The terminal allows the merchant or their client to swipe, insert, or hold a card near the device to capture the information. They are often connected to point-of-sale systems so that paymentamounts and confirmation of payment can betransferred automatically to the merchant'sretail management system.

## 4.4 NFC Chip

NFC is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1½ in) of each other.


***Fig. 3. NFC chip***

NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards and allow mobile payment to replace or supplementthese systems. This is sometimes referred to as NFC/CTLS (contactless) or CTLS NFC. NFC is used for social networking, for sharing contacts, photos, videos or files. NFC-enabled devices can act as electronic identity documents and keycards. NFC offersa low-speed connection with simple setup that can be used to bootstrap more capable wireless connections.

NFC is a short-range wireless communication technology enabling data exchange between devices over distances typically less than 10 cm. NFC chips are embedded in credit cards, smartphones, and other IoT-enabled devices for secure, contactless transactions.

NFC chips capture transaction details such as amount, timestamp, and merchant information and transmit this data to IoT systems.

NFC technology employs encryption protocols (e.g., AES, DES) and tokenization to protect sensitive transaction data during transmission.

By connecting to IoT gateways or smartphones, NFC devices enable real-time monitoring and data

aggregation for further analysis by Generative AI models.

Technical Specifications

### 4.5 Communication Protocols

NFC operates under ISO/IEC 14443 and ISO/IEC 18092 standards.

It supports active and passive modes, enabling device-to-device and card-to-reader communication.

Passive NFC chips derive power from the electromagnetic field generated by the NFC reader, eliminating the need for a battery. A tamper-resistant hardware component within the chip safeguards sensitive data. Advanced encryption standards prevent eavesdropping and relay attack are used for Cryptographic methods.

## 5. Challenges and Mitigations

**Security Risks:** Susceptible to skimming and relay attacks.
**Mitigation:** Use of tokenization and mutual authentication protocols.
**Limited Range:** Restricted to short distances, making scalability challenging.
Mitigation: Deployment of NFC-enabled IoT hubs for localized data collection.
**MongoDB, Data Model:** BSON (Binary JSON) format supports hierarchical data storage, allowing complex transaction data to be efficiently managed.
**Horizontal Scalability:** Sharding enables the database to distribute data across multiple servers, accommodating the high-velocity, high-volume IoT data streams.
**Indexing:** Supports complex queries with optimized indexes, such as geospatial indexes for location-based fraud analysis.
**Replication:** Ensures high availability and fault tolerance through replica sets, maintaining data integrity in distributed environments.
**Security Features:** Encrypted data storage and Secure Socket Layer (SSL) for secure communication.
RBAC to enforce data access permissions.

### 5.1 Advantages of the Proposed System

- **Real-Time Detection:** Combines IoT's real-time monitoring with AI's predictive capabilities.
- **Improved Accuracy:** Reduces false positives by employing advanced Generative AI models.
- **Scalability:** Cloud integration supports large-scale financial networks.
- **Enhanced Security:** IoT encryption and secure communication protocols protect transactional data.
- This architecture ensures a seamless, accurate, and secure mechanism for detecting and mitigating credit card fraud in real-time.
- The proposed system architecture leverages IoT devices and Generative AI models to create a robust, scalable, and adaptive credit card fraud detection framework. Below are the key components and their interactions:

### 5.2 Advantages in Fraud Detection

**High Performance:** Optimized for read and write operations in real-time fraud detection scenarios.
**Flexibility:** Handles dynamic data structures, essential for storing varied IoT transaction attributes.
**Integration with AI Pipelines:** MongoDB seamlessly integrates with AI frameworks like TensorFlow and PyTorch for model training and anomaly detection.

### 5.3 Query Optimization Tools for Generative AI

- Complex queries on large datasets can degrade performance.
- Mitigation: Implementation of effective indexing and aggregation pipelines.

## 6. Experimental Results

### 6.1 Anaconda IDE (Jupyter Notebook)

Jupyter Notebook, formerly known as IPython Notebook, is a web-based interactive computing environment that enables users to create and share documents containing live code, equations, visualizations, and narrative text. The term "notebook" may refer to the Jupyter web application, the

underlying Jupyter server, or the notebook document format itself, depending on the context. A Jupyter Notebook document is structured as a JSON file adhering to a versioned schema and consists of an ordered sequence of input/output cells. These cells can include executable code, Markdown-formatted text, mathematical expressions, plots, and other rich media, and are typically saved with the ".ipynb" file extension.

### 6.2 Logistic Regression

Logistic regression is a type of statistical modeling technique used primarily for binary classification tasks. It applies the logistic function to estimate the probability that a given input belongs to one of two categories. In the context of regression analysis, it involves determining the parameters of a logistic model, which is particularly useful when the dependent variable is dichotomous—for example, outcomes like "pass" or "fail." These binary outcomes are typically represented using indicator variables, with the two possible classes denoted by "0" and "1".

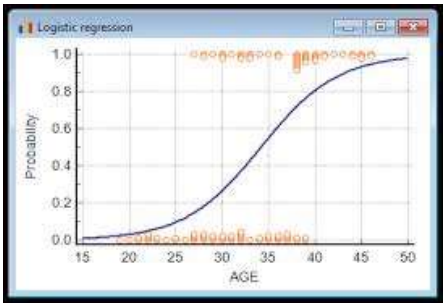


***Fig. 4.*** *Logistic Regression*

## 7. Conclusion

Fraud detection has long been a vital and evolving area of research, driven by the continuous emergence of new fraud patterns. This work presents a novel approach to detecting credit card fraud by identifying four distinct patterns of fraudulent behavior through the application of carefully selected and fine-tuned machine learning algorithms. Our system incorporates predictive analytics and a real-time notification mechanism via a graphical user interface (GUI), alerting users immediately upon detection of suspicious activity.

At the core of the proposed solution are Near Field Communication (NFC) technology and MongoDB. NFC enables secure, real-time capture of transaction data, while MongoDB offers the flexibility and scalability necessary to store and manage large volumes of IoT-generated data used for model training and fraud analysis. This integration strengthens the system's capacity to detect fraudulent transactions promptly and accurately.

The system is designed with IoT integration to enhance transaction security and reduce the likelihood of fraud, making it a distinctive contribution to the field. By enabling real-time detection and providing actionable insights, the system supports fraud investigation teams in making timely decisions. The methodology also includes the use of resampling techniques to address data imbalance, which significantly improves classifier performance. The machine learning models implemented in this study achieved promising accuracy rates of 74%, 83%, 72%, and 91% for the respective fraud patterns, demonstrating the effectiveness of the proposed approach.

## Compliance with Ethical Standards

**Conflicts of interest:** Authors declared that they have no conflict of interest.

**Human participants:** The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

## References

[1] Jisha Shaji, Dakshata Panchal," ImprovedFraud Detection in e-Commerce Transactions", 2024 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA)

[2] John Richard D. Kho, Larry A. Vea," CreditCard Fraud Detection Based on TransactionBehavior", Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2020

[3] John O. Awoyemi," Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach" Published in *Big Data and Cognitive Computing, MDPI, 2024*.DOI: 10.3390/bdcc8010006
[4] Suman Arora, Dharminder Kumar," Selectionof Optimal Credit Card Fraud Detection Models Using a Coefficient Sum Approach", International Conference on Computing, Communication and Automation (ICCCA2017)
[5] CCFD-GAN: Credit Card Fraud Detection Based on Generative Adversarial Networks, I*EEE Xplore*. DOI: Available through IEEE Digital Library, DOI: 10.3390/bdcc7010007
[6] Sonali Bakshi," Credit card fraud detection Aclassification Analysis"
[7] Mrs. C. Navamani, M. Phil, S. Krishnan,"Credit Card Nearest NeighborBased Outlier Detection Techniques"
[8] En.wikipedia.org. (2020). Credit card fraud.[online]Available at:https://en.wikipedia.org/wiki/Credit_card_fraud [Accessed 24 Jan.2020]
[9] Mittal H (2014) Diffie-Hellman based smart-card multi-server authentication scheme. Sixth International Conference on Computational Intelligence and Communication Networks. https://doi.org/10.1109/CICN.2014.173.9.
[10] Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Trans Inf Forensics Secur 10:1953–1966.https://doi.org/10.1109/TIFS.2015.243996410.
[11] Ruhul A, Hafizul Islam SK, Karati A (2016) Design of an enhanced authentication protocol and its verification using AVISPA. Recent Advances in Information Technology.https://doi.org/10.1109/RAIT.2016.750793611.
[12] Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng2017:25. https://doi.org/10.1155/2017/9324035
[13] Abdellatif R, Aslan HK, Elramly SH (2011) New real time multicast authentication protocol. International Journal of Network Security 12:13–20. https://doi.org/10.1016/j.ejrs.2011.11.003.2.
[14] Armando A, Basin D, Boichut Y (2005) The AVISPA tool for the automated validation of internet security protocols and applications. International Conference on Computer Aided Verification 3576:281–285.https://doi.org/10.1007/11513988_273.
[15] Chang CC, Wu HL, Wang ZH, Mao Q (2013) An efficient smart card based authentication scheme using image encryption. J Inf Sci Eng 29:1135–11504.
[16] El-Emam E, Koutb M, Kelash H, Faragallah OS (2011) An authentication protocol based on Kerberos 5.International Journal of Network Security 12:159–1705.
[17] He D, Chen J, Hu J (2011) Weaknesses of a remote user password authentication scheme using smart card.International Journal of Network Security 13:58–606.
[18] Hwang MS, Chong SK, Chen TY (2010) Dos-resistant ID-based password authentication scheme using smart cards. J Syst Softw 83:163–172. https://doi.org/10.1016/j.jss.2009.07.050