International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0208
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1273 - 1277

A Systematic Credit Card Analysis for Detection of Compromised Data Using Machine Learning

prof. Pradeep S Ingle[1], Samiksha Sandip Borkar[2], Karan Pradip Morey[3], Harshwardhan Tejrao Pawar[4], Om Vishwanath Vasu[5]

[1]Assistant Professor, IT Department, Anuradha Engineering College, Chikhli, Buldhana, Maharashtra, India.

[2,3,4,5]Student, Anuradha Engineering College, Chikhli, Buldhana, Maharashtra, India.

Email ID: *samikshaborkar41@gmail.com[2], karanmorey106@gmail.com[3], harshpawar9323@gmail.com[4], omvasu143@gmail.com[5]*

Abstract

Credit card security is paramount for banks, especially during the pre-issuance phase. This paper examines the multifaceted security measures implemented by banks to protect credit cards and cardholder data before a card is even issued. We explore the vulnerabilities inherent in the card production and personalization processes, and analyze the various countermeasures employed to mitigate these risks. These include secure printing facilities, data encryption, EMV chip technology integration, and rigorous access controls. Furthermore, we discuss the importance of robust data security protocols for safeguarding sensitive information during application processing and account setup. This paper highlights the proactive approach taken by banks to minimize the potential for fraud and data breaches in the critical pre-issuance stage, ensuring the integrity and security of the credit card ecosystem. The findings emphasize the continuous need for vigilance and innovation in security practices to stay ahead of evolving threats and maintain customer trust.

Keywords: *Security, Data, Encryption, Protocols, Threats*

1. Introduction

Data on Cloud, with its on-demand access to shared resources like software, platforms, storage, and information, has transformed IT infrastructure. However, this shared environment is vulnerable to various security threats. This paper comprehensively reviews simulation techniques used to evaluate the impact of such attacks focusing specially on credit card related fraud. We examine different attack types, available simulation tools, and key metrics for assessing security. Furthermore, we propose a novel framework for credit card issue process by bank that integrates existing approaches while addressing their limitations. This framework will assist researchers and practitioners in designing and executing effective simulations to enhance issue of non-compromise credit cards. Because vulnerabilities related to credit card provides a virtual pool of resources, confidentiality, integrity, availability, authenticity, and privacy are critical concerns for both providers and consumers. These security concerns have spurred active research due to the numerous threats organizations face. This work provides a concise yet thorough analysis of data security and privacy issues at banker side, discusses current solutions, and outlines future research directions in this vital area.

2. Objectives

- To demonstrate the generation of credit card number and its comprise result for attacks to simulate the attacks through multiple profile
- To identify the difference of previous, comprise of card numbers and current
- To generate the comprise numbers and stored for Record in Cloud Through Encryption Process [1-3]

3. Problem Statement

Every bank always needs to provide security to the customer vulnerable data and by virtue of which all bank is secured, but still there are some of the issues existed even though with high security configuration. The issue of credit card is one of the most excessive

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0208
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1273 - 1277

frauds generated at baker level and this need to reduce by using today's updated technology. During issue of credit card, the number generated by the card was created by some random logic, but if we compare the generated credit card with the compromise fraud data so that it is easy to reduce the fraud on credit card. This study was presented in this paper and the technique used to reduce it. [4-6]

4. Literature Review

Mousa st.al. states that cybersecurity is experiencing significant technological development, and the changes have been driven by its operations in recent years. The secret to creating an intelligent and automated security system is to extract patternsor insights from cybersecurity data and create a matching data-driven model. One of the main problems, and threats to information security, is fraud. Credit card fraud detection (CCFD) is a significant issue for consumers, businesses, and banks, mostly because of the growth of computerized financial transactions. Because of this, a methodology for detecting fraud is presented that uses state-of-the-art machine learning (ML) techniques. The methodology in this research is a carefully chosen set of state-of-the-art ML algorithms that are particularly made for accurate CCFD problems. The technique uses a wide range of ML models to handle large-scale problems with a large number of transactions. Three ML models are used in this study, such as logistic regression (LR), random forest (RF), and XGBoost. These models are trained for accurate results of CCFD. Four evaluation metrics are used in this study to evaluate the ML models, such as accuracy, precision, recall, and f1 score. The results show that the RF model has the highest accuracy of 99.65%, followed by the XGBoost, with 99.963% accuracy, and the LR model, with 99.934% accuracy. The study's summary gives banking organizations, governmental organizations, and legislators crucial knowledge to help them fight against the harm that credit card theft does to customers, businesses, and the economy at large. By offering an ML-driven solution to the fraud problem, our work solves it and opens the door for further advancements in this important field. Credit card fraud has changed significantly because of the growing use of electronic payment methods. In the past, neither rule-based nor signature-based methods have been able to keep up with the ever-evolving tactics used by scammers [3-4]. The startlingly high incidence of credit card theft continues to be a significant issue for individuals, businesses, and financial institutions alike. In the face of the increasingly sophisticated strategies employed by fraudsters, rule-based systems, and static patterns, the foundation of traditional fraud detection techniques—is insufficient[5-6 [1] Patil et. al. states that detecting credit card fraud is a major social issue. Credit card usage on e-commerce and banking websites has quickly expanded in recent years. The usage of credit cards in online transactions has made it simple, but it has also increased the frequency of fraud transactions. Modernization will have both beneficial and negative effects. It is always encouraged for banks and e-commerce sites to have automatic fraud detection systems as part of the operations taking place. Huge financial losses could be the outcome of credit card theft. Machine learning approaches offer good answers when searching for ways to stop credit card fraud from happening. When compared to other algorithms currently being used, the proposed system achieves greater accuracy by using a random forest application to solve the issue. All of the fundamental classifiers have the same weight, but the random forest algorithm has a relatively high weight while the others have relatively low weights due to the fact that the bootstrap sampling of decision-making and attribute selection cannot be guaranteed to be equally stable across all classifiers. Credit card payments, cardless purchases via Google Pay, PhonePe, Samsung Pay, and PayPal are all common in daily life. The detection of fraud, which results in a significant financial loss each year, is a current issue. The scam is predicted to reach double digits by 2020 if it keeps going in this direction. The fact that the card is no longer physically necessary to complete the exchange has led to an increase in extortion transactions. The economy is impacted emotionally by fraud discovery [1]. Fraud detection is essential and necessary in this approach. To combat this issue, financial institutions must use a variety of fraud detection tools. But over

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0208
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1273 - 1277

time, scammers find ways to get around the strategies put in place by business owners. Fraud detection continues to increase and it remains a serious worry in society despite all the preventive measures taken by financial institutions, strengthening of law, and government doing their best efforts to eradicate fraud detection. Credit cards are frequently used in the expansion of Internet commerce, mobile applications, and particularly in web-based transactions. [2] Hafez1et. al. states that the rapid increase of fraud attacks on banking systems, financial institutions, and even credit card holders demonstrate the high demand for enhanced fraud detection (FD) systems for these attacks. This paper provides a systematic review of enhanced techniques using Artificial Intelligence (AI), machine learning (ML), deep learning (DL), and meta-heuristic optimization (MHO) algorithms for credit card fraud detection (CCFD). Carefully selected recent research papers have been investigated to examine the effectiveness of these AI-integrated approaches in recognizing a wide range of fraud attacks. These AI techniques were evaluated and compared to discover the advantages and disadvantages of each one, leading to the exploration of existing limitations of ML or DL-enhanced models. Discovering the limitation is crucial for future work and research to increase the effectiveness and robustness of various AI models. The key finding from this study demonstrates the need for continuous development of AI models that could be alert to the latest fraudulent activities. The internet has grown astonishingly in the face of rapidly changing technological advances like big data, software-defined networking, and cloud computing. Nevertheless, serious cybersecurity risks are associated with these developments, which significantly impact essential infrastructure. Traditional safety techniques have found it challenging to keep up with the sophistication of new cyber-attacks since they rely on fixed safety mechanisms like intrusion prevention and fraud system detection. DL has become a disruptive force that opens new opportunities for improved performance, data accessibility, and further optimization. It has not only revolutionized voice, image, and behavioral analytic applications in AI, but it has also brought revolutionary developments in robotics, speech recognition, and facial recognition. DL has been developed as a crucial tool in cybersecurity for malware monitoring and intrusion detection. Compared to previous ML applications, this represents a significant advancement. While ML has demonstrated some potential, its dependence on human characteristic extraction has been verified to be problematic, particularly in cybersecurity. [3]

5. Credit Card Security at Banking Side

To protect credit cards and cardholders from fraud and data breaches, banks use a comprehensive, multi-layered security approach. This involves several key strategies, including: [7-10]

- Secure Card Production: Manufacturing takes place in tightly controlled, monitored facilities. Cardholder data is encrypted during personalization, and EMV chip technology is incorporated to make transactions more secure.
- Transaction Protection: Banks verify cardholder identity and card validity during transactions using methods like Figure 1 shows Flow of the Proposed System

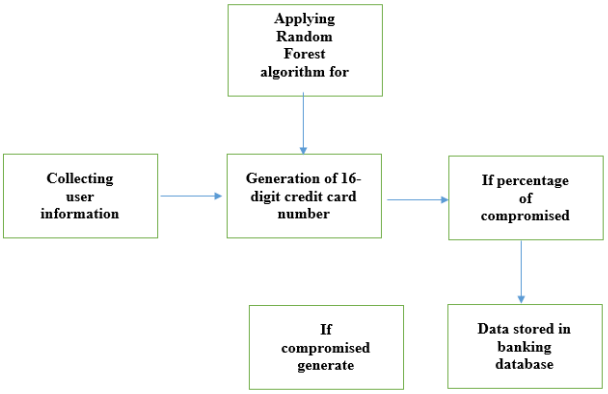

Figure 1 Flow of the Proposed System

- **Step 1: (Data Preparation):** Credit card information has been sent to the server over the network. The information is a 46-digit string formed by concatenates some values such as Credit card number, card verification value and expiry date of the card. For the purpose of security, the information has been

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0208
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1273 - 1277

encrypted before sent to server over the network. The encryption technique used for securing the cipher text is Caesar cipher. Caesar cipher has been used with shift value of three. Original string of 46 digits has been converted into encrypted string of same length. For the purpose of security of Credit card application, some of the network attacks have been examined. An attack has been examined on the credit card information being sent over the network. [11-13]

- **Step 2: Implement RF Classifier:** Random forest classifier creates a set of decision trees from a randomly selected subset of the training set. It is a set of decision trees (DT) from a randomly selected subset of the training set and then It collects the votes from different decision trees to decide the final prediction
- **Step 3: Training and Testing For Model Creation:** The selected ML algorithm learns how to make predictions or categorize data using the training set. In this phase, the model refines its internal settings to best match the training set of data. Finding the optimal values for hyperparameters (parameters that govern the learning process) that are not learned from the data is known as "hyperparameter tuning." In order to enhance the performance of the model, we are experimenting with various hyperparameter settings using the validation set.
- **Step 4: Implement Enhanced RF Classifier:** In this step, we will prepare the data by standardizing it, separating features from labels, and then splitting it into training and validation sets for machine learning model development and evaluation.
- **Step 5: Test Result with Different Metrics:** This stage allows us to identify the comprise value of credit card and stored on cloud so as to maintain the records for future references

Conclusion

In conclusion, while data security computing has revolutionized IT infrastructure by offering on-demand access to shared resources, it simultaneously introduces significant security vulnerabilities, particularly concerning sensitive data like credit card information. This paper has provided a comprehensive review of simulation techniques designed to assess the impact of attacks targeting these vulnerabilities, with a specific focus on credit card fraud. By examining various attack types, simulation tools, and key security metrics, and by proposing a novel framework for credit card issuance that addresses the limitations of existing approaches, this work aims to empower researchers and practitioners to develop more robust and secure systems. This framework, designed to simulate attacks and enhance the issuance of non-compromised credit cards, is crucial given the virtual pool of resources and inherent vulnerabilities associated with cloud environments. Ultimately, addressing the critical concerns of confidentiality, integrity, availability, authenticity, and privacy for both providers and consumers requires continuous research and development of effective security solutions. This work contributes to that ongoing effort by analyzing data security and privacy issues related to credit card issuance within the banking sector, discussing current solutions, and outlining future research directions to ensure the ongoing security and integrity of credit card transactions in the cloud era.

Reference

[1]. Mahmoud Abdallah M. M. Mousa, ―Credit Card Fraud Detection in the Banking Sector: A Comprehensive Machine Learning Approach for Information Security‖, Artificial Intell. Cyb.Vol. 2(2025) 1–13
[2]. Tejaswini Patil, Kiran Khadare, ―Credit Card Fraud Detection‖, Online ISSN: 2395-602X (www.ijsrst.com)
[3]. Ibrahim Y. Hafez, Ahmed Y. Hafez, Ahmed Saleh, Amr A. Abd El-Mageed, Amr A. Abohany, ―A systematic review of AI-enhanced techniques in credit card fraud detection‖, Journal of Big Data (2025) 12:6 Parkar P, Bilimoria A. A survey on cyber security IDS using ML methods. 2021 5th International Conference on Intelligent
[4]. Computing and Control Systems (ICICCS),

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0208
e ISSN: 2584-2854
Volume: 03
Issue:04 April 2025
Page No: 1273 - 1277

pp. 352–360, 2021. https:// api. seman ticsc holar. org/ Corpu sID: 23520 8042.

[5]. Musa N, Mirza N, Rafique S, Abdallah A, Murugan T. machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions. IEEE Access. 2024. https:// doi. org/ 10. 1109/ ACCESS. 2024. 33608 68.

[6]. Eswaran M, Hamsanandhini S, Lakshmi KI. Survey of cyber security approaches for attack detection and prevention.

[7]. Turk J Comput Math Educ. 2021;12(2):3436–41. https:// www. proqu est. com/ schol arly-journ als/ survey-cyber-security-appro aches-attack-detec tion/ docvi ew/ 26246 98524/ se-2.

[8]. Barik K, Misra S, Konar K, Fernandez-Sanz L, Koyuncu M. Cybersecurity deep: approaches, attacks dataset, and comparative study. Appl Artif Intell. 2022. https:// doi. org/ 10. 1080/ 08839 514. 2022. 20553 99.

[9]. Morovat K, Panda B. A survey of artificial intelligence in cybersecurity. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 109–115. https:// doi. org/ 10. 1109/ CSCI5 1800. 2020. 00026.

[10]. Rauf U, Mohsen F, Wei Z. A taxonomic classification of insider threats: existing techniques, future directions & recommendations. J Cyber Secur Mobil. 2023;12(2):221–52. https:// doi. org/ 10. 13052/ jcsm2 245-1439. 1225.

[11]. Thanh Vu SN, Stege M, El-Habr PI, Bang J, Dragoni N. A survey on botnets: incentives, evolution, detection and current trends. Future Internet. 2021. https:// doi. org/ 10. 3390/ fi130 80198.

[12]. Abu Bakar A, Zolkipli MF. Cyber security threats and predictions: a survey. Int J Adv Eng Manag IJAEM. 2023;5:73. https:// doi. org/ 10. 35629/ 5252-05027 33741.

[13]. Parizad A, Hatziadoniu CJ. Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework. IEEE Trans Smart Grid. 2022. https:// doi. org/ 10. 1109/ TSG. 2022. 31763 11.