Artificial Intelligence in Cybersecurity

Journal Homepage: sciencesforce.com/aics

Artificial Intell. Cyb. Vol. 2 (2025) 1–13

Paper Type: Original Article

Credit Card Fraud Detection in the Banking Sector: A Comprehensive Machine Learning Approach for Information Security

Mahmoud Abdallah M. M. Mousa [1,2,*]

[1] Faculty of Law, Ain Shams University, Cairo 11566, Egypt;

[2] Business Administration, The Arab Academy for Management, Banking and Financial Sciences (AAMBFS), Egypt; mahmoud.mousa@student.aambfs.edu.eg.

Received: 13 Aug 2024 **Revised**: 16 Dec 2024 **Accepted**: 07 Jan 2025 **Published**: 09 Jan 2025

Abstract

In the context of computers, 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 patterns or 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.

Keywords: Information Security; Credit Card Fraud Detection; Machine Learning; Cyber Security; Intrusion Detection.

1 | Introduction

Credit card fraud detection (CCFD) is a pervasive issue that impacts consumers, businesses, and financial institutions worldwide in the current digital era. Because fraudulent operations are becoming more complex and varied, sophisticated and trustworthy fraud detection systems are required, and these systems must be able to identify fraudulent activity. This work introduces a novel approach to credit card fraud detection by utilizing the potential of Machine Learning (ML). By combining state-of-the-art ML algorithms, the goal is to create fraud detection systems that are more accurate, productive, and flexible[1-2].

Corresponding Author: mahmoud.mousa@student.aambfs.edu.eg

https://doi.org/10.61356/j.aics.2025.2459

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].

Conventional methods for identifying fraud are based on static patterns and rule-based systems. A novel approach that makes use of machine learning's (ML) potential to increase the precision, effectiveness, and flexibility of fraud detection is desperately needed as fraud patterns get more intricate and dynamic[7-9].

The main contributions of this study are:

- Our study pioneers the evaluation of different ML models for CCFD. This study can help banks and organizations to eliminate financial crimes with highly accurate results.
- Our study introduces a set of challenges in information security and a set of solutions to overcome these challenges and limitations.
- Three ML models are applied in a large number of transactions for the CCFD dataset.
- Our models obtained higher accuracy and precision from the CCFD dataset.

The rest of this study is organized as follows: Section 2 shows the information security solutions and risks; Section 3 shows the materials and methods which show the full details of the steps of this study. Section 4 shows the results of ML models. Section 5 shows the conclusions of this study.

2 | Information Security

Electronic information security (IS) can be an asset for any firm, organization, or government. This information is very important for users and organizations and can be lost by attackers in digital communication. IS has various advantages in our digital world but it has various threats every time. The most important solutions of IS are cyber security and risk management [10-11].

Cyber security is a collection of technologies, methodologies, and actions of people to help in the protection and safety of IS. Cyber attackers are the most threatening to sensitive digital information. One of the highest security risks in the world is information sharing through mobile networks. The first step in assessing the system's security or risks is to define the resources in this system. Also, identifying the methodology is the best suited for risk situations. This methodology can predict the threats and identify them through a set of steps hence helping organizations and government to protect their sensitive information and data. This methodology can depend on the target of attacks and transactions in case of attacks. So, AI is the best methodology to predict cyber-attacks to prevent them and increase the security of information. Machine learning and deep learning models can be used for intrusion detection, malware classification, and cyber threat sensing [12, 13].

2.1 | Solutions for Protecting Information using ML Models

Every day, new threats and vulnerabilities are changing in network security. ML models protect against these new threats. ML models can be used for instruction detection and anomaly detection. Instruction detection refers to using ML models to identify the intrusion and prevent it before damaging the system. Anomaly detection can identify the anomalies in the network system. ML models can identify malicious attacks by searching for unusual patterns.

Software-defined network-based (SDN-based) detection systems built on ML models or cloud systems. It can convert the targeted virtual computers into safe virtual computers. ML models can enable the systems to learn from past experiences and use the collected information and knowledge to make decisions in the future. It can detect the patterns which indicate the attacks by the attackers. ML models can make alerts when detecting any malicious, prevent it, and inform humans to act [14, 15].

2.2 | Challenges of Information Security

Cyber-attacks refer to an attacker who can steal, change, and remove information in the system and organization. One of the common cyber-attack scenarios is to access confidential data in the system as a human. Cyber-attack refers to the vulnerabilities in the system and network. A cyber-attack is a scenario when several vulnerabilities take advantage of a system or network weakness. It might be difficult to become familiar with new technology, security trends, and threat intelligence. The target may have a mechanism in place to handle some cyberattacks, even if it may not be aware of all of them. Depending on its risk analysis, a cyberattack may have been caused by an inherent risk or a residual risk [16-17].

2.3 | Cyber-attack Defense

Systems for risk management and cybersecurity are built on cyberattack defenses. The primary characteristic of any IS model is how it addresses defenses against cyberattacks. Anyone who uses a variety of electronic gadgets to share a network environment can use the always-expanding cyberspace as a platform. But there are also malicious attackers and unauthorized users in cyberspace. For this reason, when it comes to cyber-attack defenses, a precautionary approach is required. An effective defense mechanism recognizes the threat or attack, notifies the system, and takes appropriate action to lessen it. The term "cyber-attack defense" refers to a collection of specified protocols and actions that may be taken as preventative measures or implemented during or following a cyberattack. It looks for indications of a successful, ongoing, or pending cyberattack. Finding the most effective cyberattack defense strategy can be aided by a retrospective analysis [18, 19].

2.4 | Problems of Information Security

The complexity and difficulties of maintaining electronic data have significantly increased in recent years. The intricacy arises from the pervasive and multipurpose nature of IS, which aims to preserve and rely on information assurance to protect an organization's valuable assets while simultaneously promoting business interactions by fostering collaboration platforms, business alliances, and trust.

To completely resolve this issue, we have determined that the following three critical management issues must be addressed:

- Addressing hazards after the entire system has been developed, undermines system security.
- Designing information and security systems concurrently.
- Using insufficient reasoning to develop solutions[20].

2.5 | Cyber security

Understanding various cyberattacks and creating defense plans that protect the properties listed below are the focus of cybersecurity.

- A property called confidentiality is used to stop information from being accessed and revealed to unapproved people, organizations, or systems.
- Integrity is a quality that keeps information from being altered or destroyed without authorization.
- Availability is a feature that guarantees an authorized entity prompt and dependable access to information assets and systems.

The phrase "cybersecurity" can be categorized into several common areas and is used in a wide range of applications, from mobile computing to business. These include: information security, which primarily considers security and the privacy of pertinent data; application security, which considers keeping the software and devices free of risks or cyber threats; network security, which primarily focuses on protecting a computer network from cyber attackers; and operational security, which covers the procedures for managing and safeguarding data assets. Network security systems and computer security systems with firewalls, antivirus programs, or intrusion detection systems make up typical cybersecurity systems[21-22].

2.6 | Risks of Security

Any attack's usual risks consider three security factors: threats, who is attacking; vulnerabilities, or the holes they are targeting; and impacts, or what the assault does. Any action that jeopardizes the availability, confidentiality, or integrity of information assets and systems is considered a security event. Several kinds of cybersecurity incidents could put a person or an organization's systems and networks in danger.

Unauthorized access refers to the practice of gaining unauthorized access to data, networks, or systems, which violates security policies.

Malware, also referred to as malicious software, is any software or program that is purposefully made to harm a computer, client, server, or computer network, such as botnets. Computer viruses, worms, Trojan horses, adware, ransomware, spyware, malicious bots, and more are examples of many forms of malware. Ransomware, often known as ransom malware, is a new type of virus that stops users from accessing their devices, personal files, or systems and then requests an anonymous online payment to unlock them.

By overloading the target with traffic that causes a crash, a denial-of-service attack aims to bring down a computer or network and render it unavailable to its intended users. A distributed denial-of-service (DDoS) attack floods the targeted resource using numerous computers and Internet connections, whereas a denial-of-service (DoS) assault usually employs a single computer with an Internet connection.

Phishing is a type of social engineering that involves a wide range of malicious activities carried out through human interactions. The fraudulent attempt involves posing as a trustworthy person or entity via electronic communication, such as an email, text message, or instant message, to obtain sensitive information, such as login credentials, banking and credit card details, or personally identifiable information.

The threat of an unidentified security flaw for which the patch has not been made available or the program developers were not aware is referred to as a "zero-day attack."

2.7 | Solutions to Information Security

2.7.1 | Protection from Firewalls

One network security strategy that helps shield computer networks from harmful activity and unauthorized access is firewall protection. An untrusted external network, like the internet, is separated from a trusted internal network by a firewall. Incoming and outgoing network traffic is monitored, and pre-established rules are applied to permit packets according to their protocol, source, destination, and other variables[23-24].

Software or hardware can be used to implement firewalls. Software firewalls are installed on individual devices, such as laptops and smartphones, whereas hardware firewalls are physical devices that are usually positioned between the internal network and the internet. To decide whether to accept or block network packets, both kinds of firewalls analyze them and compare them to a list of pre-established rules.

2.7.2 | Security of Endpoints

Protecting individual devices, including PCs and smartphones, against malware and other threats is the goal of endpoint security. Intrusion Prevention System, device management, encryption, and antivirus and anti-malware software are all included.

2.7.3 | Software for Antivirus

An essential part of cybersecurity, antivirus software helps shield systems and devices against viruses, malware, and other harmful threats. It looks for and gets rid of any possible risks by scanning files, documents, and data on a computer or network. The market offers a wide range of antivirus software choices, each with unique features and functionalities.

Finding and eliminating different kinds of malware, such as viruses, worms, Trojan horses, ransomware, spyware, and adware, is the main goal of antivirus software. These harmful applications have the potential to seriously harm a system by stealing confidential data, corrupting data, or interfering with regular system operations.

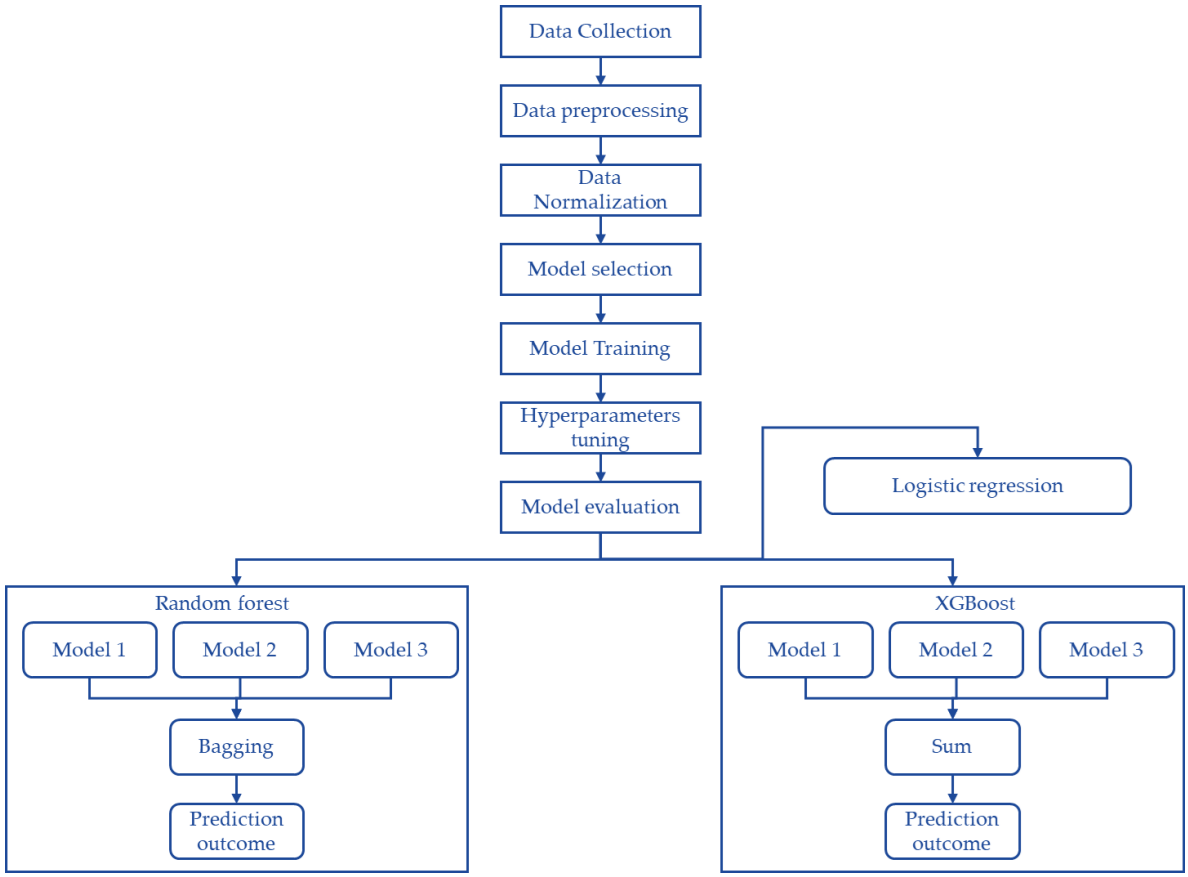

Figure 1. The flowchart of this methodology.

3 | Materials and Methods

In this section, we show the steps of the strategic framework and technical approach for the CCFD problem using AI models. We used the AI models to construct an accurate and strong system for CCFD. This section provides a comprehensive overview of our study design selecting AI models, constructing experimental study, and ethical considerations. Also, our study can solve the challenges and problems in the CCFD database such as null value, outliers, biased data, and participant confidentially. Figure 1 shows the flowchart of our study to show the efficiency and effectiveness of our AI models.

3.1 | Dataset Collection

We collect the dataset of CCFD from the Kaggle website for applying the ML models for high accuracy and precision. This dataset is used for different reasons such as having large numbers of rows and transactions, completeness, and has different goals for the CCFD problem. This dataset has large numbers of transactions with legitimate and fraudulent ones.

Figure 2 shows the number of transactions fraud and the number of transactions has no fraud. Figure 3 shows the time feature of the dataset.

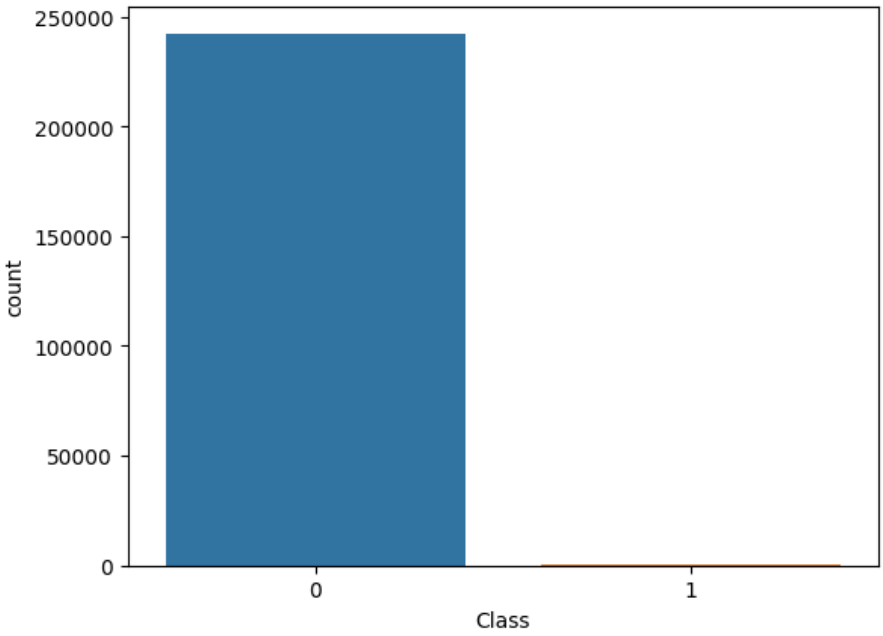

Figure 2. The number of transactions.

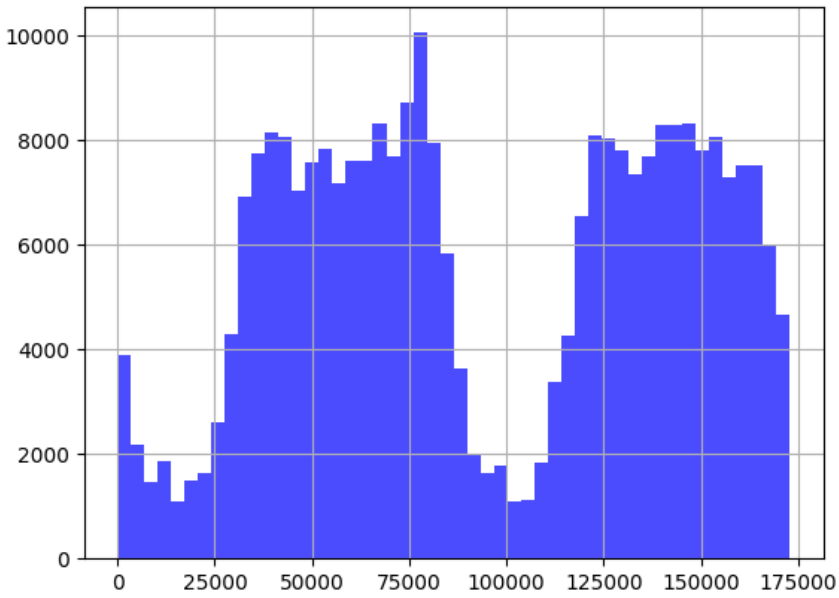

Figure 3. The time feature.

3.2 | ML Models

This part shows the details of three ML models to implement for the CCFD problem.

3.2.1 | Logistic Regression

Logistic Regression (LR) is a supervised learning model used for classification problems. It can predict the probability to belong of class or not. It can analyze the relationship between features of the dataset. It can predict the results of categorical dependent variables [25-26].

3.2.2 | Random Forest

Random Forest (RF) is a powerful tree-learning model that uses a decision tree algorithm to train data and obtain accurate results. It creates different decision trees in the training stage, each tree working on random sample data. Then it can combine the results of all trees by voting in the classification task. It can reduce the risk of overfitting and enhance the overall prediction performance [27, 28].

3.2.3 | XGBoot

XGBoost is a gradient-boosting library that is used to obtain high accuracy and precision in classification problems. It is an ensemble model. It aggregates different weak models to produce stronger models for the best prediction output. It has different advantages in ML models such as the ability to obtain higher accuracy and performance and the ability to deal with large amounts of datasets with accurate results. It can deal with missing values without requiring extra data processing steps in ML processing. It can train large amounts of data in a short time due to it working on parallel processing [29, 30].

3.3 | Evaluation Matrix

Evaluating the performance of ML models in CCFD problems is critical for ensuring high accuracy and precision. This part shows different evaluation metrics such as:

$$\text{Accuracy} = \text{A} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$$

$$\text{Precision} = \text{B} = \frac{\text{TP}}{\text{TP+FP}}$$

$$\text{Recall} = \text{C} = \frac{\text{TP}}{\text{TP+FN}}$$

$$\text{F1} - \text{score} = \text{D} = \frac{2*\text{B}*\text{C}}{\text{B+C}}$$

4 | Results

In this study, we show the outcomes of our methodology in the use of ML models for CCFD dataset evaluation. Our objective is to train the different ML models to detect fraud or not in the CCFD dataset. We used three ML models in this study such as LR, RF, and XGBoost. Different metric evaluations are used to evaluate three ML models to show the limitations and advantages of each model.

4.1 | LR Results and Performance

The advantages and effectiveness of LR models in defining the CCFD transactions. The LR correctly classified around 99.934% of transactions with an accuracy of 99.934%. LR had a precision of 82.857% meaning that 82.857% of the transactions it flagged as potentially fraudulent were indeed fraudulent. RF has around 74.358% recall whereas the ability of the model to identify 74.358% of all occurrences of fraud. RF has 78.378% f1 score results where the results were nearly identical in terms of precision and recall. In summary, LR had better results and performance in evaluating CCFD. Figure 4 shows the LR results, and Figure 5 shows the confusion matrix. Figure 6 shows the classification report.

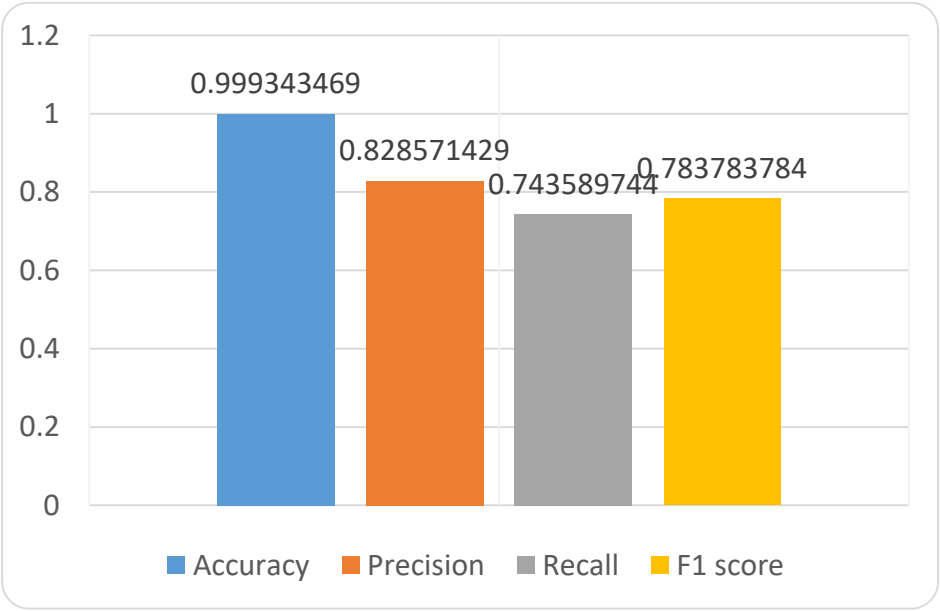

Figure 4. LR Metrices results.

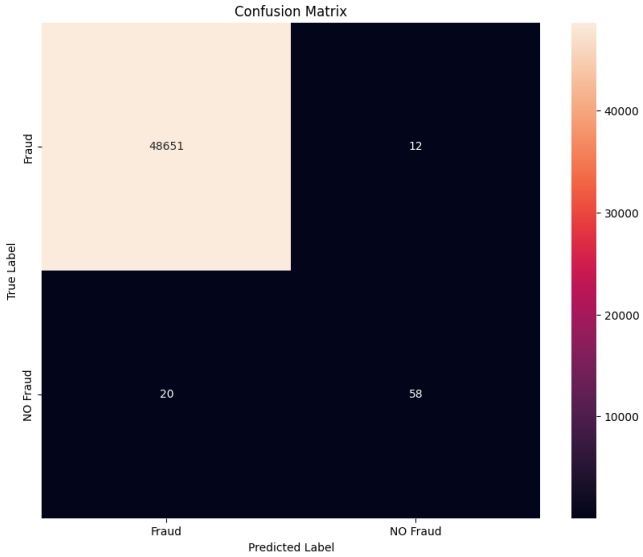

Figure 5. LR confusion matrix.

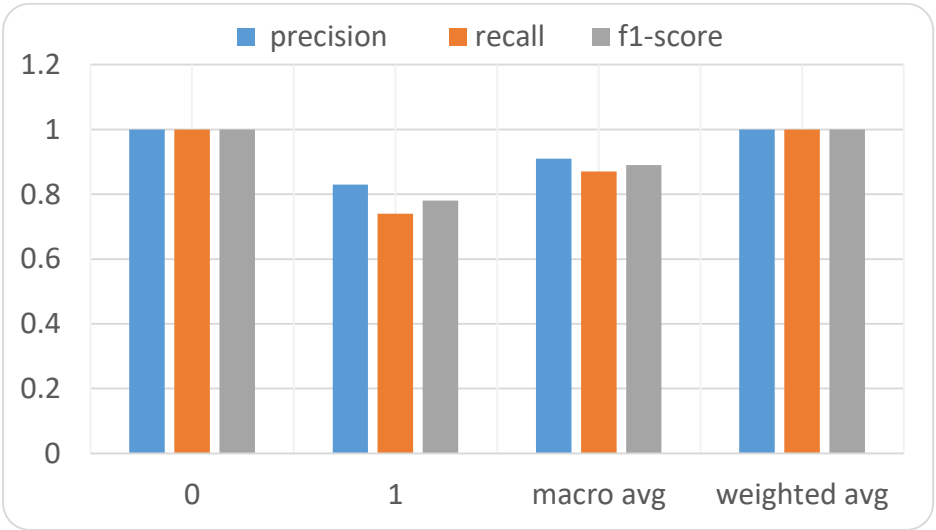

Figure 6. LR Classification report.

4.2 | RF Results and Performance

The advantages and effectiveness of RF models in defining the CCFD transactions. The RF correctly classified around 99.965% of transactions with an accuracy of 99.965%. RF had a precision of 94.203% meaning that 94.203% of the transactions it flagged as potentially fraudulent were indeed fraudulent. RF has around 83.333% recall where the ability of the model to identify 83.333% of all occurrences of fraud. RF has 88.435% f1 score results where the results were nearly identical in terms of precision and recall. In summary, RF had better results and performance in evaluating CCFD. Figure 7 shows the RF results, and Figure 8 shows the confusion matrix. Figure 9 shows the classification report.

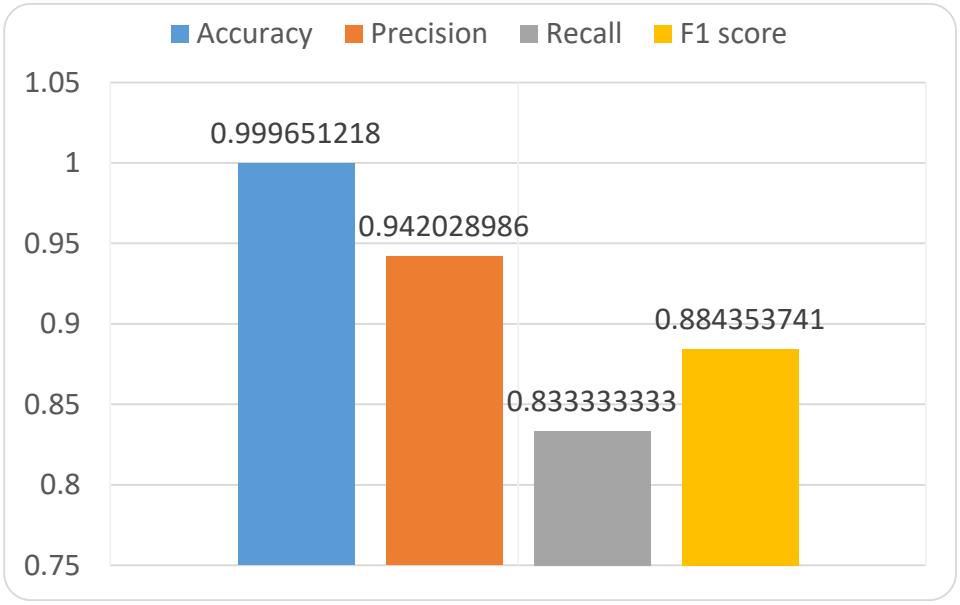

Figure 7. RF Matrices results.

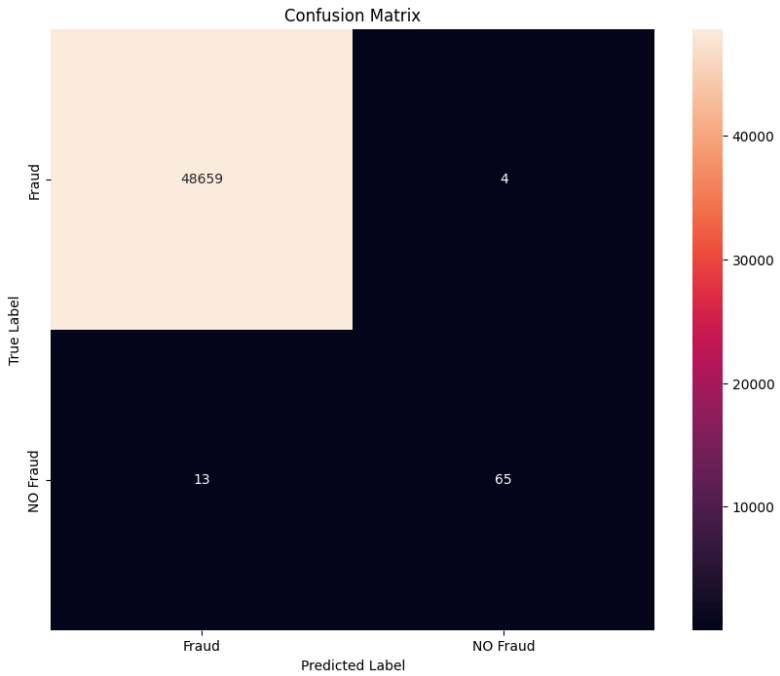

Figure 8. RF confusion matrix.

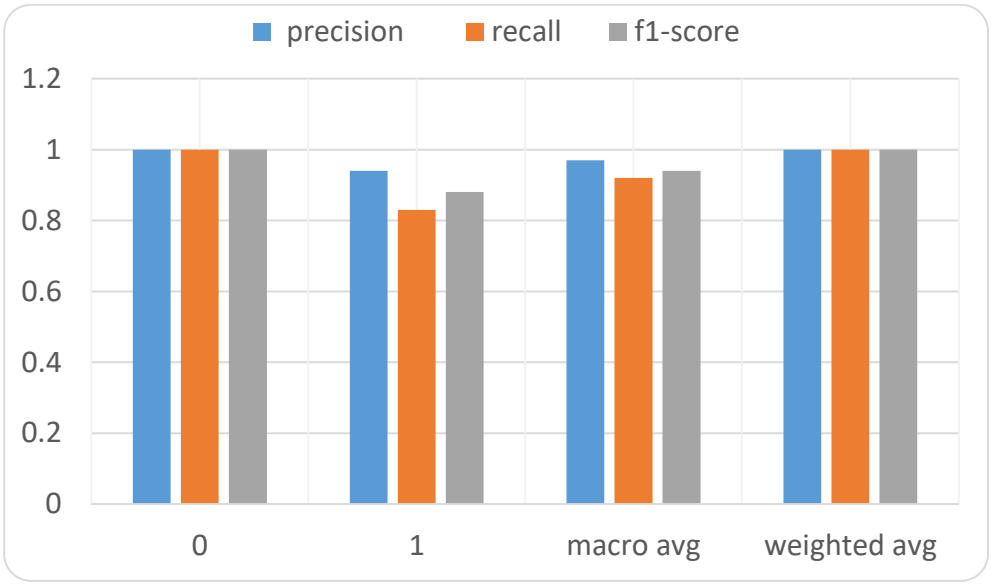

Figure 9. LR Classification report.

4.3 | XGBoost Results and Performance

The advantages and effectiveness of XGBoost models in defining the CCFD transactions. The XGBoost correctly classified around 99.963% of transactions with an accuracy of 99.963%. XGBoost had a precision of 91.667% meaning that 91.667% of the transactions it flagged as potentially fraudulent were indeed fraudulent. XGBoost has around 84.615% recall where the ability of the model to identify 84.615% of all occurrences of fraud. XGBoost has 88.0% f1 score results where the results were nearly identical in terms of precision and recall. In summary, XGBoost had better results and performance in evaluating CCFD. Figure 10 shows the XGBoost results, and Figure 11 shows the confusion matrix. Figure 12 shows the classification report.

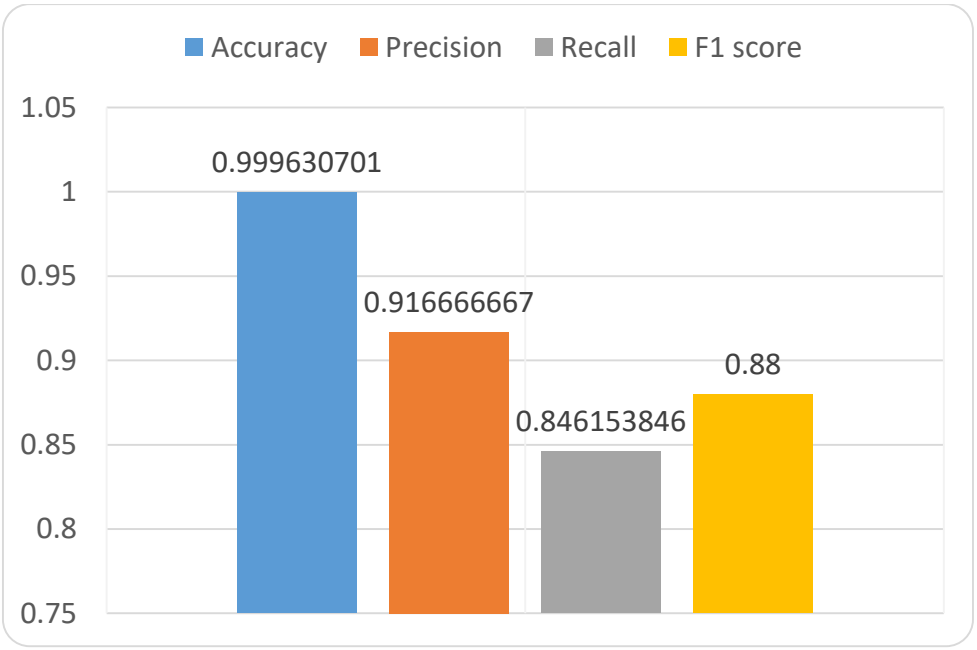

Figure 10. XGBoost metrices results.

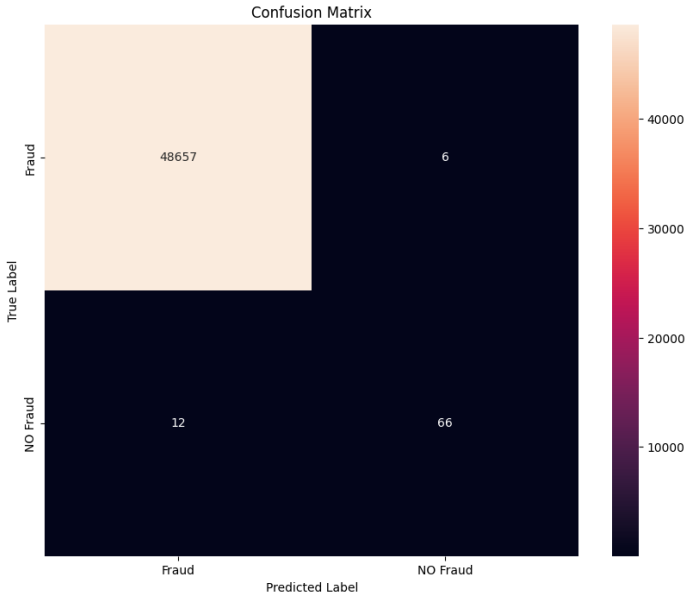

Figure 11. XGBoost confusion matrix.

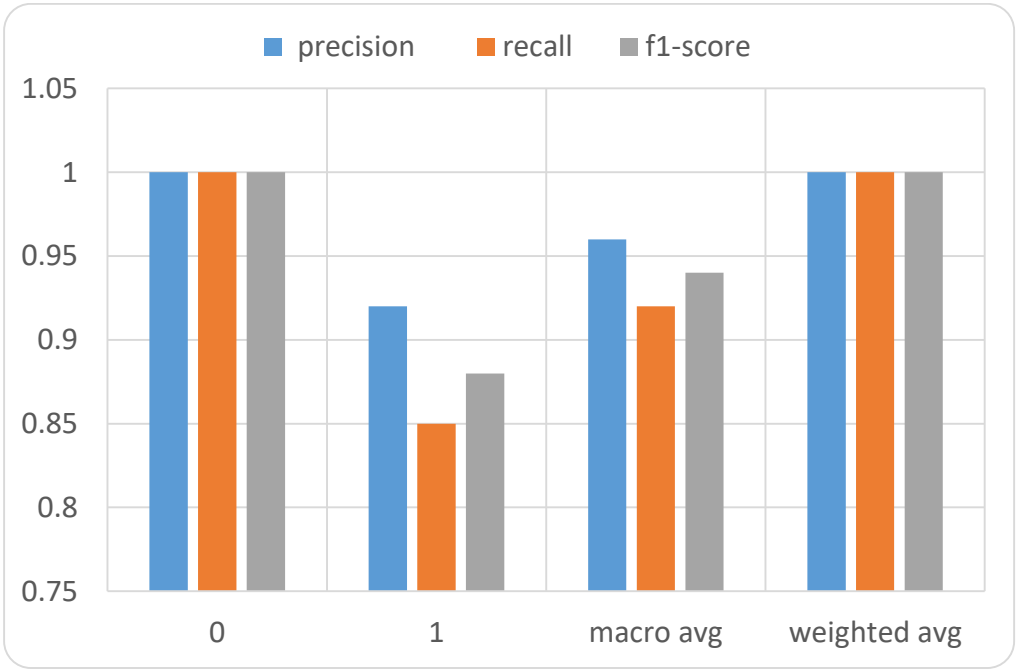

Figure 12. XGBoost classification report.

4.4 | Comparative Model Analysis

This part shows the comparative analysis results of three ML models that are used to evaluate the CCFD dataset as shown in Table 1.

Table 1. Three ML models result.

ML	Accuracy	Precision	Recall	F1 Score
LR	0.99934	0.82857	0.74359	0.78378
RF	0.99965	0.94203	0.83333	0.88435
XGBoost	0.99963	0.91667	0.84615	0.88

We show the RF model has the highest accuracy in the classification of fraud transactions in the CCFD dataset. RF has the highest precision score. XGBoost model has the highest recall score. We show the RF has the highest f1 score.

5 | Conclusions

This study demonstrates how well-sophisticated machine-learning algorithms identify CCFD. Our comparison of Random Forest, XGBoost, and Logistic Regression shows that ensemble-based models—Random Forest and XGBoost in particular—perform better at detecting fraudulent transactions in a range of real-world situations. These models are useful tools for financial institutions trying to improve their fraud detection systems because of their high accuracy, precision, and recall. They are particularly well-suited for managing intricate fraud patterns in real-time.

Our results highlight the significance of implementing cutting-edge machine learning approaches, both to increase the precision of fraud detection and to guarantee that systems are adaptable enough to take advantage of emerging fraud trends. To protect against the increasing risks of digital financial crimes, financial institutions, governmental organizations, and legislators may use these insights to create fraud detection systems that are more secure, dependable, and responsive.

To sum up, the suggested machine learning-based method establishes a new benchmark for the detection of fraud and opens the door for more study and advancement for security systems. The financial sector can keep ahead of increasingly skilled fraudsters and shield customers and institutions from any threats by consistently enhancing these models and integrating cutting-edge technology.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] M. N. Alatawi, "Detection of fraud in IoT based credit card collected dataset using machine learning," Mach. Learn. with Appl., vol. 19, p. 100603, 2025.

[2] K. Chaudhary, J. Yadav, and B. Mallick, "A review of fraud detection techniques: Credit card," Int. J. Comput. Appl., vol. 45, no. 1, pp. 39–44, 2012.

[3] S. Lakshmi and S. D. Kavilla, "Machine learning for credit card fraud detection system," Int. J. Appl. Eng. Res., vol. 13, no. 24, pp. 16819–16824, 2018.

[4] L. Delamaire, H. A. H. Abdou, and J. Pointon, "Credit card fraud and detection techniques: a review," Banks Bank Syst., vol. 4, no. 2, 2009.

[5] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in 2017 international conference on computing networking and informatics (ICCNI), IEEE, 2017, pp. 1–9.
[6] N. K. Trivedi, S. Simaiya, U. K. Lilhore, and S. K. Sharma, "An efficient credit card fraud detection model based on machine learning methods," Int. J. Adv. Sci. Technol., vol. 29, no. 5, pp. 3414–3424, 2020.
[7] K. Fu, D. Cheng, Y. Tu, and L. Zhang, "Credit card fraud detection using convolutional neural networks," in Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III 23, Springer, 2016, pp. 483–490.
[8] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Human-Centric Intell. Syst., vol. 2, no. 1, pp. 55–68, 2022.
[9] Y. Jain, N. Tiwari, S. Dubey, and S. Jain, "A comparative analysis of various credit card fraud detection techniques," Int. J. Recent Technol. Eng., vol. 7, no. 5, pp. 402–407, 2019.
[10] M. Stamp, "A survey of machine learning algorithms and their application in information security," Guid. to vulnerability Anal. Comput. networks Syst. an Artif. Intell. approach, pp. 33–55, 2018.
[11] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, "Machine learning security: Threats, countermeasures, and evaluations," IEEE Access, vol. 8, pp. 74720–74742, 2020.
[12] C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," Sensors, vol. 22, no. 5, p. 2017, 2022.
[13] M. Stamp, Introduction to machine learning with applications in information security. Chapman and Hall/CRC, 2022.
[14] V. Ford and A. Siraj, "Applications of machine learning in cyber security," in Proceedings of the 27th international conference on computer applications in industry and engineering, IEEE Xplore Kota Kinabalu, Malaysia, 2014.
[15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," IEEE access, vol. 8, pp. 222310–222354, 2020.
[16] Y. Miao, C. Chen, L. Pan, Q.-L. Han, J. Zhang, and Y. Xiang, "Machine learning–based cyber attacks targeting on controlled information: A survey," ACM Comput. Surv., vol. 54, no. 7, pp. 1–36, 2021.
[17] A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," Soft Comput., vol. 25, no. 18, pp. 12319–12332, 2021.
[18] D. L. Bergin, "Cyber-attack and defense simulation framework," J. Def. Model. Simul., vol. 12, no. 4, pp. 383–392, 2015.
[19] M. M. Yamin and B. Katt, "Use of cyber attack and defense agents in cyber ranges: A case study," Comput. Secur., vol. 122, p. 102892, 2022.
[20] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," J. Big data, vol. 7, pp. 1–29, 2020.
[21] G. Apruzzese et al., "The role of machine learning in cybersecurity," Digit. Threat. Res. Pract., vol. 4, no. 1, pp. 1–38, 2023.
[22] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," Cogent Eng., vol. 10, no. 2, p. 2272358, 2023.
[23] J. Liu, "Enhancing Network Security Through Router-Based Firewalls: An Investigation into Design, Effectiveness, and Human Factors," Highlights Sci. Eng. Technol., vol. 85, pp. 724–732, 2024.
[24] R. K. Kolli, E. Priyanshi, and S. Gupta, "Palo Alto Firewalls: Security in Enterprise Networks," Int. J. Eng. Dev. Res. 12 (3), 1-13. rjwave ijedr/viewpaperforall. php? Pap. IJE DR200A001, 2024.
[25] A. Das, "Logistic regression," in Encyclopedia of Quality of Life and Well-Being Research, Springer, 2024, pp. 3985–3986.
[26] M. S. Chowdhury, M. N. Rahman, M. S. Sheikh, M. A. Sayeid, K. H. Mahmud, and B. Hafsa, "GIS-based landslide susceptibility mapping using logistic regression, random forest and decision and regression tree models in Chattogram District, Bangladesh," Heliyon, vol. 10, no. 1, 2024.
[27] Z. Sun, G. Wang, P. Li, H. Wang, M. Zhang, and X. Liang, "An improved random forest based on the classification accuracy and correlation measurement of decision trees," Expert Syst. Appl., vol. 237, p. 121549, 2024.
[28] J. Rafapa and A. Konokix, "Ransomware detection using aggregated random forest technique with recent variants," 2024.
[29] M. Niazkar et al., "Applications of XGBoost in water resources engineering: A systematic literature review (Dec 2018–May 2023)," Environ. Model. Softw., p. 105971, 2024.
[30] S. Luo, B. Wang, Q. Gao, Y. Wang, and X. Pang, "Stacking integration algorithm based on CNN-BiLSTM-Attention with XGBoost for short-term electricity load forecasting," Energy Reports, vol. 12, pp. 2676–2689, 2024.