International Journal of Future Engineering Innovations

Credit Card Fraud Detection Using a Proposed Model: "Blockchain Technology

Oluwatomisin Arokodare [1*], Dr, Hayden Wimmer [2], Dr. Yiming Ji [3]
[1-3] Department of Information Technology, Georgia Southern University, Statesboro GA, USA

* Corresponding Author: **Oluwatomisin Arokodare**

Article Info

ISSN (online): 3049-1215
Volume: 02
Issue: 04
July – August 2025
Received: 08-05-2025
Accepted: 09-06-2025
Published: 03-07-2025
Page No: 11-18

Abstract
Credit card security and fraud are increasing concerns as we move towards a cashless society. Credit card data breaches represent a significant risk and a growing amount of economic loss across the globe. Many aspects of credit cards make retailers and banks vulnerable to fraud and in the case of merchants, customer loss. Blockchain is a potential solution to mitigate this credit card fraud.
Expanding on this approach, fraudulent credit card transactions caused by intermediate parties would be reduced with the help of a proposed blockchain solution with fraud detection technologies. This technology will increase transparency between banks and their customers while also preventing fraud before it occurs, helping institutions avoid losing millions to fraud-related losses.
Our conceptual model implements a federated and coordinated central blockchain branching into personal blockchains which are protected via two factor authentication. This work focuses on sophisticated methods for securing credit card information, eliminating the burden and risk of credit card fraud activities by an unauthorized party, and ensuring that only the issuers and the user of the credit card knows what it is, this will significantly minimize the likelihood of credit card fraud.

DOI: https://doi.org/10.54660/IJFEI.2025.2.4.11-18

Keywords: Credit card, Security, Business fraud, Security of Credit card, Data, Credit card fraud detection, financial institution Credit card information, Blockchain, Data Leakages

1. Introduction

Traditional credit card payments are not safe from credit card fraud because persistent attackers can readily figure out a secret credit card number. Providing a credit card to an anonymized person, including a server or cashier, escalates the likelihood of identity theft or the chance of the card number being recorded, captured, and perhaps even scanned, which can conclude in alleged involvement. Many traditional payment methods are ineffective for online transactions. Cash, money orders, and checks are impractical methods of payment, although some firms are implementing their own direct-payment networks to circumvent this restriction, electronic cash transfers still require direct knowledge of the sending and receiving bank accounts. There is a significant danger associated with this excellent simple method of making transactions. The most popular payment method is credit cards, which are not restricted by rules and are utilized in about 95% of online transactions.

Credit cards, bank accounts, and other financial instruments are increasingly being targeted by organized criminal groups in the cyber environment for fraudulent activities. Credit cards are not the panacea that we may hope for, a sharp rise in credit card fraud has been associated with increased credit card use electronically, and users must diligently review their transaction records to be aware they are being defrauded. It is crucial to protect credit card information from getting into the wrong hands, but no viable solution appears to exist to ensure the card's safety whether it is securely slotted in the owner's wallet or when it is used by a 3rd party [1]. Lack of security can result in the vulnerability of credit card numbers stored in online databases, which is another problem, it is fraught with problems. Credit cards can be swiped through readers to prevent them from being physically handled, the new chips in the card make the situation worse because hackers can now obtain card information without having to physically handle the card by scanning it with wireless readers while the card is safely stored in a wallet.

Private or sensitive information on credit cards could be revealed to unauthorized individuals, which results in an unintended or accidental leak of credit card data, and there may be significantly more serious repercussions if such data is lost due to hacking or malware. A certain threshold or limit can be implemented on the credit card; this will trigger a voice confirmation in systems that the card is used and identify transactions that seem to deviate from the owner's monthly card usage pattern by using logical patterns.

The remaining part of this paper is divided into 5 sections; The background of the research topic is presented in section II. Related works are presented in section III. Our methodology for securing credit card information from data leakages is shown in section IV. Section V shows the discussion of different techniques for securing card information from data leakage and fraud. The conclusion of the research work is presented in section VI.

2. Background

Credit card transactions have vastly increased in number due to globalization and the increased adoption of the internet for online shopping. Even though these payment methods have many benefits, such as the ability to quickly purchase any item and pay later, they also carry several security threats. Credit card fraud turns into a nightmare for everyone involved because losses from credit card fraud are rising. The security of a credit card is based on the silicon card's physical security as well as the confidentiality of the card's number. There are two different kinds of credit cards: physical cards and virtual cards. When making a purchase with a physical card, the user is required to present the card. If a fraudulent user of this kind wants to access his or her card, he only needs to steal that card [2].

Customer/Cardholder: The person making the purchase with a credit card issued by the card's issuer.

- **Issuer:** The financial organization (bank, for example) that provides the card to the cardholder. Payment for authorized transactions is guaranteed by the issuer.
- **Merchant:** The merchant provides the goods and services and has a financial agreement with the acquirer.
- **Acquirer:** The merchant's financial institution that manages the authorizations and payments for credit card transactions.

The fraudulent use of a virtual card must be aware of specific credit card information, including the credit card details, Card verification number, and security pin [3]. Credit card theft occurs when an unauthorized person obtains the credit card details, or personal unique Identifier and uses it to make purchases in stores, online, or over the internet without the owner's knowledge. Furthermore, the individual using the credit card has no connection to the cardholder or issuer and has no intention of disclosing the purchase to the cardholder or paying back the purchase price. We have two types of credit card fraud: offline fraud and online fraud. The usual method of identifying offline fraud is to use a stolen credit card to purchase any goods at a store. On the other hand, online fraud (cardholder-not-presents) occurs through mail, telephone, and internet orders.

The risk of fraudulent card activity affects approximately all or some of the parties involved. Customers are the party that is least affected, this is because of the legislation that is in place in most countries restricting the customer's liability for credit card transactions. Most laws impose fines on merchants for any losses brought on by fraud, particularly when a card is not physically present. Cardholders have a policy in place called cardholder protection that covers most of the cardholder losses. To initiate a chargeback for the disputed amount, the card issuer will submit a chargeback to the merchant (via the acquirer) to reverse the credit for the transaction whenever the customer objects to any transaction made using their credit cards. It will be impossible to reverse the chargeback if the merchant is unable to offer any proof (e.g., proof of delivery) to the acquirer. Furthermore, the merchant will bear all costs, including the price of the items, delivery, transaction bank fees, and chargeback fees. However, the consequences of fraud may sometimes be borne by the Issuer or Acquirer (Bank). In a situation when the Issuer/Acquirer is not paying the direct cost of the fraud, they will inevitably be responsible for paying some indirect charges.

There are operational and manpower charges that the bank must pay, just like in the event of chargebacks made to the merchant. Issuers and acquirers must also invest heavily in credit card fraud prevention by employing advanced IT systems for detecting fraudulent transactions. In this paper, we will explore some approaches for securing credit card information from fraudulent activities, this will put the cardholder in power and provides them with the ability to decide the minimum payment and transaction time, thereby securing their credit card information [3].

One of the primary objectives of information security is to prevent data from being disclosed to unauthorized parties. To reduce the risk of credit card information being leaked, this continuously propels the financial sectors to research, develop, and build various security measures. The need to access and use credit card information necessitates the unavoidable release of sensitive data, making it impossible to constantly prevent data leakage. This information breach may be caused by intentional action or an unintentional error. Monitoring user activity is a key component of credit card fraud detection since it allows for the estimation, detection, and prevention of undesirable behavior. Understanding the mechanisms used to detect credit card theft and being able to recognize the fraud is essential for effectively mitigating this crime.

3. Related Works

According to recent research by Nassar, N. and G. Miller [4], credit card information leakage is growing in both the public and private sectors of society, several cardholders make use of credit card activation to trace deviation from their usual routine and legal transaction. However, the system will detect and raise an alert for illegal transactions since it was far from the user's normal pattern. Credit card information can be secured by using temporary credit card numbers that are electronic, this can be done without disclosing a user's actual credit card number. The user must use a physical credit card with restrictions when they are at a place of business, such as an eatery, so these capabilities are therefore unavailable to them. However, silicon credit cards facilitate the hacking process by allowing hackers to swipe their stylish card readers on top of their wallets and get all card information. There is a need to secure the way credit cards are used and confidently ensure individual card information won't be accessed by the wrong person or an illegitimate user, a secure payment process is required in obtaining authorization and

restricting approved transaction limits for genuine credit card transactions. The account holder will define one or more constraints for each transaction, and the actual transaction is only those that comply with these restrictions.

Bhatla, T.P., V. Prabhu, and A. Dua [5], identified that an existing card that was obtained illegally can be tampered with by deleting the metallic strip with a strong electro-magnet. After that, the fraudster then tampers with the card's details to make them match those of a legitimate card, which they may have obtained from a stolen till roll. The cashier will repeatedly swipe the card through the machine until the fraudster starts using it, at which point they will realize that the metallic strip is inoperative. The cashier will then proceed to manually enter the card information into the device. This type of fraud has a high risk because the cashier will extensively scrutinize the card to read the numbers, which poses a high threat to credit card fraud.

According to Kou, Y., *et al*. [6], the difficulties in sharing ideas make it difficult to create credit card information detection systems. The tools for detecting fraud can be applied in a variety of ways, including data mining, statistics, and artificial intelligence. The methods for detecting fraud fall into two categories: supervised methods and unsupervised methods. In supervised approaches, we must create a model utilizing examples of both fraudulent and non-fraudulent transactions and train the model to distinguish between the two. Therefore, if a new transaction occurs, this model should be able to classify it into one of the two types. The supervised techniques can also only be used to identify certain types of fraud. To verify the compatibility of the fraudulent transaction, the credit card company immediately verifies the number with the generated number in their system. If they are identical, the verification code is returned to the merchant; if not, a rejection code is sent.

Raj, S.B.E. and A.A. Portia [7] proposed the use of a hidden Markov model which is a double-embedded stochastic process. This model indicates that if an incoming credit card transaction has a sufficiently high probability and is not accepted, it is a fraudulent transaction. The model is trained with the normal behavior of a credit cardholder. Each transaction is submitted for verification, showing the details and the value to determine if the transaction is legitimate or not, and receives the card details and the purchase amount. When the detection system detects a fraudulent transaction, it alerts the issuing bank, and the transaction is rejected. The cardholder concerned might then be contacted and informed that the card might have been misused. This model produces high false positive and false alarm rates.

Bentley, P.J., *et al*. [8] highlighted that the fuzzy Darwinian detection system employs evolutionary programming to create fuzzy logic rules that may categorize credit card transactions into “suspicious and non-suspicious” ones, making it possible to detect stolen cards and frauds more quickly. An accumulation of fuzzy rules with varying lengths evolved using genetic programming. The transaction is classified as normal when the customer's payment is on time or when the number of past-due payments is fewer than three months; otherwise, it is classified as abnormal. They implemented custodial authorization, in which the customer communicates with the credit card issuer about the payment. The card issuer would inquire about the cardholder's security and the customer simply provides the merchant with the invoice number in return. This shows that the merchant has been identified, the credit card account has been identified, and one of the several previously established payment categories has been designated.

Maes, S., *et al*. [9, 10] proposed the Bayesian approach as an automatic solution for detecting credit card fraud using machine learning. Bayesian networks, commonly known as belief networks, are a type of artificial intelligence programming that uses several techniques, such as machine learning algorithms and data mining, to generate layers of data or beliefs. Bayesian networks are capable of processing data as required without the prerequisites for testing when employing supervised learning. When incoming data is ambiguous or partially unavailable and some information is known beforehand, Bayesian belief networks are particularly successful at simulating the situation. To identify patterns and classify data, this knowledge or opinion is used.

Mareeswari, V. and G. Gunasekaran [11] proposed hybrid support vector machine technology to perform credit card fraud detection at the beginning of the credit card application process. This method predicts widespread fraud and illegal conduct. This method makes use of the hybrid support vector machine (HSVM) to compute the weight of each characteristic for communal and spike detection for credit card application fraud detection to detect frauds. The primary goal of this system is to address the problems caused by the shortcomings of the current system, such as adaptability, rapid response times, efficiency, data imbalances, inaccurate predictions, etc. The initial stage of the credit card life cycle is to identify the fraudulent user.

4. Methodology

It's easy for retailers to feel victimized and vulnerable given all the negative effects of fraudulent credit card operations, including financial and nonfinancial losses, fines, loss of reputation, etc. The lengthy period between the time a fraudulent transaction takes place and the time it is discovered, or when the cardholder starts a chargeback, is one of the major challenges with credit card fraud prevention. The average time between the transaction date and the chargeback notification, according to statistics, may be up to 72 days. This means that, in the absence of credit card fraud protection measures, one or more fraudsters could easily cause major harm to a person or business before the concerned entity is aware of the issue. However, there is a need for technological advancements in preventing credit card information from data leakage and fraud. The various preventive techniques are discussed below.

The proposed technique for protecting credit card information from data leakage combines the distinct features of a credit card used in a physical place with secure transaction features which are easily accessible. The method starts by retaining the user's credit card information in Bluetooth or internet smartphone or another mobile device. The mobile device acts as the purchasing mechanism, thus in a way, it's like having a digitized wallet. The approach integrates the characteristics of a credit card used in a store with online secure transaction features. The credit card information retained on the portable device is a certificate authority that recognizes the user, and their banking provider as opposed to a credit number [4]. The credit card or credentials are never disclosed to the waiter or to anyone else whenever the user utilizes the credit card in an eatery or anywhere.

The technology is presented to the smartphone of the user utilizing a digital device and sharing transaction-related

information stored over an encrypted channel. A transient credit card number to use for the payment must be requested from the credit provider via the user's device. The time-limited card number is then linked to a specific merchant for a fixed amount, a defined date, and perhaps a specific time. The merchant receives this time-limited number and conducts transactions as normal. The information provided by the user and the merchandise information delivered to the creditor must match. Other possible applications for this method include Point of Sale terminals, where a consumer checking out at a retail outlet might use their smartphone device to communicate with the Checkouts to complete the transaction rather than disclosing their credit card by scanning it through the reader [4].

Another technique that can be used in securing credit cards from fraud is the use of cardholder authentication, which is a new technology [12, 13]. The methodology is based on biometrics which saves a cardholder's distinctive traits such as a fingerprint or the way they sign their names so that a computer can read it. Biometrics can be linked to credit cards and provide a secure direct authentication channel between the customer and the issuing bank. When the cardholder enrolls for the credit card, the bank issues a PIN associated with a thumbprint authentication, this will only be used to authorize transactions. The next generation of personal identity verification systems appears to be based more on biometrics which enables the identification of a person through the verification of distinctive physical or behavioral traits. To help identify the card's legitimate owner, fingerprints offer a secure and distinctive connection between the cardholder and the personal information on the document. The ability to authenticate a person's identification via their biometrics is strengthened because they cannot be borrowed, lost, or stolen like a PIN. Fingerprint security ensures that only the rightful cardholder has permitted access to the personal information stored inside the card. There are several different kinds of biometrics systems being developed, including dynamic signature verification, hand-based verification, retinal and iris scanning, and fingerprint verification. When a transaction is performed by a cardholder the issuing bank will request for their password and biometric validation, after the two have been validated, the merchant can proceed with the transaction and forward the validation data to their acquirer. The acquirer will carry out a check with the customer issuing bank and request for authentication code to complete the transaction [12].

Neutral network technology can possibly spot fraudulent transactions immediately to lessen the severity of any losses brought on by credit card fraud [14, 15]. This technique has been developed to analyze customer spending habits and to warn individuals of the presence of unauthorized transactions, as well as merchant deposit monitoring techniques to detect the claiming patterns of dishonest merchants. They are implemented on statistical information that may be found in huge databases of past transactions, notably fraudulent ones. These neural network models can link and weigh several fraud indications such as unusual transaction size and credit card history, to the occurrence of fraud because they have effectively been trained using examples of both genuine and fraudulent transactions. The principles of neural networking are inspired by how the brain works, specifically pattern recognition and associative memory. Based on its associative memory of previously acquired patterns, the neural network can identify similar patterns and forecast future values or events. The benefit that neural networks have over other techniques is that they can learn from the past and hence improve results over time. Using the current circumstance as a starting point, they can also derive rules and forecast future behavior. Banks can quickly and effectively identify fraudulent card transactions by using neural networks.

In securing credit card transactions from data leakages, a negative list and positive list card be initiated by the merchant [16]. A negative list is a database used to spot high-risk transactions based on data fields. A negative list, which is designed to stop repeat offenders from committing credit fraud, might be a file holding all the credit card numbers that have resulted in chargebacks in the past. In a similar manner, a merchant can create negative lists based on billing names, street locations, emails, and internet protocols (IPs) that have resulted in fraud or attempted fraud, essentially barring any additional efforts. An acquirer or merchant may opt to review or limit orders coming from certain nations on a list of high-risk nations that it has created and keeps up to date. This list includes card numbers that could be utilized by fraudsters, such as cards that have recently been reported as lost or stolen. Positive files are frequently used to identify trusted consumers and omit some checks by using information like their card number or email address. It is an essential tool for avoiding needless delays in processing legitimate requests.

The use of time-based numbers to protect credit card information with regularly changing security numbers is important, consumers should always utilize their credit cards to make payments and pay back their amounts in full on the due date based on underlying incentives over other payment devices. However, some customers are hesitant to utilize credit cards for most of their purchases because they are concerned that they will not be able to make full payments when their credit card bills are due. The card can be divided into two parts. The magnetic strip is in the upper portion, where commercial credit card readers can read it. A silicon circuitry is present in the bottom section and is responsible for generating a fresh card number at each predetermined interval. A window with a showcase in which the new number will be displayed and a button that will start the process of generating new numbers as required.

The relationship between the security code and the date is set by the established procedure. With the aid of this predetermined procedure, a strong authentication number can be established. The system used by the credit card issuer would record the card's specified values and be capable of determining the security number given a date because the number is a result of the timestamp. Since they use the same algorithms, both the number displayed by the card issuer and the number shown in the display window are coordinated and similar. For the encrypted card number to be transmitted to the card issuer, the cardholder must enter it at the retailer's point of sale, thereby preventing their card information being exposed or leaked to unauthorized individuals [17].

5. Proposed Method

With the increased use of online payments for goods and services, the likely chance of credit card fraud has risen compared to the decade's long history of credit cards. Blockchain technology can be applied to digital asset transactions that are traded online. Blockchain systems for transactions are focused on reducing credit card frauds with an extra level of security. Blockchain with credit card fraud detection technology will assist to mitigate fraudulent credit

card transactions due to its intermediate parties. Credit cards users, issuers and merchants that accept credit cards as a form of payment will benefit from blockchain systems. The blockchain scalability solution is a description of how effectively blockchain processes network transactions. The public blockchain, which emphasizes greater security and is visible to both the client and the financial institution, will be used in this proposed blockchain system to protect credit card information and transactions from fraud. The suggested system's blockchain design will make use of a primary algorithm to protect the blockchain as well as a combination of the cryptographic algorithm SHA256 to convert and secure the fundamental findings at every level of the output. Blockchain's transparency will make it simple to establish reliable proof and expose any potential inconsistencies in credit card transactions. Financial institutions could assist in adjusting an account's credit limit based on the credit card holder's spending habits by encoding a fraud prediction model into a credit card transaction. The decentralized data processing infrastructure is built on blockchain, which has gained widespread interest worldwide. The blockchain mechanism is a ledger of arbitrary transactional records in the form of data blocks; these blocks are linear and in chronological sequence, allowing the bank to launch the smart contract with deposits and request credit card details through a secure channel to decrypt the exchanged keys; the customer then submits the credit card details and the bank either accept or reject the payment. Blockchain consensus procedures come into play by identifying the trustless nodes in accordance with the agreement on the global blockchain data state with no identity authentication and no messaging overhead.

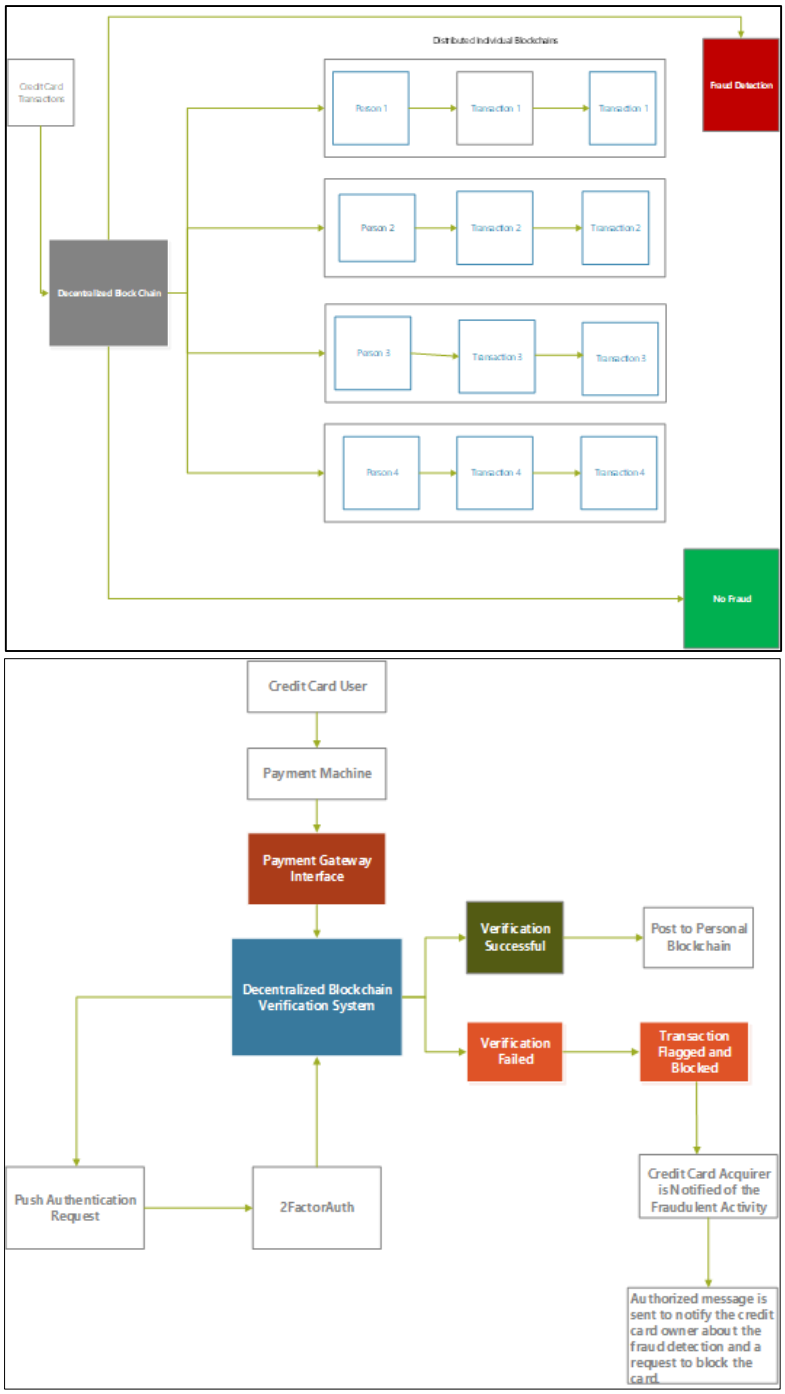

Fig 1: Credit Card Fraud Detection using proposed Blockchain Technology Workflow

6. Discussion

Credit cards are now widely used for all online payments. It is an easy form of payment for people to comprehend and feel comfortable with using. Promises of digital currency, smart cards, digital checks, and other alternative online payment methods have been entirely unfulfilled. Unfortunately, in cybercrime, where fraudsters use cutting-edge technologies to manipulate, credit cards have now become the new target. Credit cards are fraudulently and deceptively used for illegal financial advantage. In other words, to steal money from an account or to receive products without paying for them. However, due to their low storage capacity, credit cards used for electronic payments, which have become widespread, are mainly used for little sums of money. Using a credit card is anonymous and challenging to track, in contrast to using physical money. Some establishments manipulate swiping card readers to broadcast customer data across open wireless networks, and this increases the possibility of hackers using payment systems to acquire credit card information which is illegal.

Information about credit cards should only be sent between the user and the issuer, it is not necessary for the merchant or acquirer to carry out their duties. The cardholder's permission on the relevant payment is all that is required of the issuer. The issuer acquires the merchant's name from the acquirer via the current card payment infrastructure and the cardholder's transaction history can be examined to determine the cardholder's spending patterns.

7. Threats and Consequences of Using Credit Cards

There are numerous hazards and implications involved with the revealing of sensitive or personal information on transaction receipts when a credit card is used to purchase an item both online and offline. The merchant prints transaction receipts following a payment transaction, this includes releasing private information such as the truncated PAN showing only the last four digits of the card number, the card expiration date, the names of the cardholders, the card verification value (CVV), the payment brand, the approval code, and the customer signatures.

However, if the transaction is successful, the merchant will make a copy of the transaction receipts as evidence of the transaction purchase. All the sensitive information on the receipt will provide the merchant with full access to active credit card details, putting the cardholder in danger because the receipt can be used in phishing schemes to obtain complete account details and the unauthorized person can impersonate the bank or business where the purchase was made to obtain full cardholder details, the truncated credit card number should be treated as sensitive information and kept private. Criminals known as "dumpster divers" can get further information, such as names, addresses, phone numbers, or ID numbers, when these receipts are disposed of with other personal files.

When the transaction is unsuccessful, the vendor will duplicate the transaction receipts of the failed transaction purchase, having Identity thieves may be able to open false accounts and make unlawful purchases if this data is not properly destroyed. The adoption of unsecured shopping sites where the URL begins with https and no padlock is displayed beside it indicates that when sensitive information such as credit card number, card expiration date, and security code is entered, the information will not be encrypted, and this site is not safe. Providing sensitive information on this site exposes users to the risk of disclosing their information to fraudsters [18]. The benefit of utilizing payment methods like PayPal is that no one ever sees the user's credit card information while the transaction is in progress. The acquisition of the cardholder's financial data makes the cardholder the target of telemarketing. The issuer's ability to track the cardholder's purchasing patterns is limited without the merchant information.

8. Conclusion

Credit cards used for online purchases may have a big influence on banks, merchants, and cardholders. To reduce possible losses, a variety of techniques are employed to spot potential fraud. The internet has many benefits for commercial transactions, but it also has the potential for credit card transaction fraud. Securing credit card information from fraud can be conducted in a variety of methods. The structure of this method consists of a device that permits network communication between the vendor and the customer's system. A physical card or transaction is necessary when utilizing the techniques for securing credit card information to ensure the highest level of security. Additionally, the consumer can use a device to accept payment requests from the merchant, along with the requested amount and merchant ID, and send a secure request to the bank for a temporary credit card number, along with the requested amount, timeframe, and merchant, to the cardholder's device and system.

Credit cardholders should take precautionary measures to protect their credit cards, such as discarding receipts, papers, and mail containing sensitive information properly, and never providing credit card information to an unsecured or unprotected site. The risk of credit card fraud increases if credit card information is provided to anyone who requests it via SMS, email, or phone contact. A bank will never call, email, or SMS you for personal information. When using free Wi-Fi or an unreliable connection, credit cardholders should also refrain from using any online banking services or websites that save or request your credit card information. Checking monthly credit bills for unauthorized purchases is a must, as is filling out printed forms for payment methods that need full credit card information.

In this paper, techniques on how to secure physical credit cards from data leakage and fraud are discussed. The paper proposed a blockchain technology mechanism as a solution to secure credit card transactions. This will help improve how financial institutions and users handles transactions with public blockchain mechanism that is visible to all users. The cardholder's device sends the vendor's device a temporary copy of the credit card information to complete the transaction and it can be utilized with this system to give transactions requiring physical cards the highest level of security, also restricting credit card fraud.

9. References

1. Barker KJ, D'amato J, Sheridon P. Credit card fraud: awareness and prevention. Journal of Financial Crime. 2008.
2. Aigbe P, Akpojaro J. Analysis of security issues in electronic payment systems. International Journal of Computer Applications. 2014;108(10).
3. Al-Furiah S, Al-Braheem L. Comprehensive study on methods of fraud prevention in credit card e-payment system. In: *Proceedings of the 11th International

Conference on Information Integration and Web-based Applications & Services*; 2009.
4. Nassar N, Miller G. Method for secure credit card transaction. In: 2013 International Conference on Collaboration Technologies and Systems (CTS); 2013. IEEE.
5. Bhatla TP, Prabhu V, Dua A. Understanding credit card frauds. Cards Business Review. 2003;1(6):1-15.
6. Kou Y, *et al*. Survey of fraud detection techniques. In: IEEE International Conference on Networking, Sensing and Control; 2004. IEEE.
7. Raj SBE, Portia AA. Analysis on credit card fraud detection methods. In: 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET); 2011. IEEE.
8. Bentley PJ, *et al*. Fuzzy Darwinian detection of credit card fraud. In: Proceedings of the Korea Information Processing Society Conference; 2000. Korea Information Processing Society.
9. Maes S, *et al*. Credit card fraud detection using Bayesian and neural networks. In: Proceedings of the 1st International NAISO Congress on Neuro Fuzzy Technologies; 2002.
10. Brause R, Langsdorf T, Hepp M. Neural data mining for credit card fraud detection. In: Proceedings 11th International Conference on Tools with Artificial Intelligence; 1999. IEEE.
11. Mareeswari V, Gunasekaran G. Prevention of credit card fraud detection based on HSVM. In: 2016 International Conference on Information Communication and Embedded Systems (ICICES); 2016. IEEE.
12. Harris AJ, Yen DC. Biometric authentication: assuring access to information. Information Management & Computer Security. 2002.
13. Vats H, Ruhl R, Aghili S. Fingerprint security for protecting EMV payment cards. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST); 2015. IEEE.
14. Carolina A. Online credit card fraud: An emerging crime in the information technology. InFestasi. 2012;8(2):219-226.
15. Simon H. Neural Networks: A Comprehensive Foundation. Prentice Hall; 1999.
16. Baladolla EMSW, Fernando WPC, Rathnayake RMNS. Credit card fraud prevention using blockchain. In: 2021 6th International Conference for Convergence in Technology (I2CT); 2021.
17. Kaur K, Gupta I, Singh AK. A comparative study of the approach provided for preventing the data leakage. International Journal of Network Security & Its Applications. 2017;9(5):21-33.
18. Mandell L. The Credit Card Industry: A History. Twayne Pub; 1990.
19. Von Solms S. An investigation into credit card information disclosure through point-of-sale purchases. In: 2015 Information Security for South Africa (ISSA); 2015. IEEE.
20. Ghosh S, Reilly DL. Credit card fraud detection with a neural-network. In: Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences; 1994. IEEE.
21. Delamaire L, Abdou H, Pointon J. Credit card fraud and detection techniques: a review. Banks and Bank Systems. 2009;4(2):57-68.
22. Githae AN. Factors Influencing Credit Card Fraud at Equity Bank Kenya Limited [dissertation]. United States International University-Africa; 2020.
23. Lee J, Kwon KN. Consumers' use of credit cards: store credit card usage as an alternative payment and financing medium. Journal of Consumer Affairs. 2002;36(2):239-262.
24. Leonard KJ. Detecting credit card fraud using expert systems. Computers & Industrial Engineering. 1993;25(1-4):103-106.
25. Shenbagavalli R, Shanmugapriya A, Chowdary YL. Risk analysis of credit card holders. International Journal of Trade, Economics and Finance. 2012;3(3):219.
26. Cachin C, Vukolic M. Blockchain consensus protocols in the wild. IBM; 2017.
27. Anas SH, Shihab AH. Security improvement of credit card online purchasing system. Scientific Research and Essays. 2011;6(16):3357-3370.
28. Btoush E, *et al*. A Survey on Credit Card Fraud Detection Techniques in Banking Industry for Cyber Security. In: 2021 8th International Conference on Behavioral and Social Computing (BESC); 2021. IEEE.
29. Rao MLK, *et al*. A Study of fraud detection approaches in Credit Card Transactions.
30. Jing R, *et al*. Improving the Data Quality for Credit Card Fraud Detection. In: 2020 IEEE International Conference on Intelligence and Security Informatics (ISI); 2020. IEEE.
31. Ausubel LM. Credit card defaults, credit card profits, and bankruptcy. American Bankruptcy Law Journal. 1997;71:249.
32. Asha R, KR SK. Credit card fraud detection using artificial neural network. Global Transitions Proceedings. 2021;2(1):35-41.
33. Aleskerov E, Freisleben B, Rao B. Cardwatch: A neural network based database mining system for credit card fraud detection. In: *Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr)*; 1997. IEEE.
34. Yildiz M, Göktürk M. Combining biometric ID cards and online credit card transactions. In: 2010 Fourth International Conference on Digital Society; 2010. IEEE.
35. Jain AK. Biometric recognition. Nature. 2007;449(7158):38-40.
36. Vangala RR, Sasi S. Biometric authentication for e-commerce transaction. In: 2004 IEEE International Workshop on Imaging Systems and Techniques (IST); 2004. IEEE.
37. Pradhan S, Lawrence E, Zmijewska A. Bluetooth as an enabling technology in mobile transactions. In: International Conference on Information Technology: Coding and Computing (ITCC'05); 2005. IEEE.
38. Mokhtar MF, Ahmad CW, Rahman KA. E-Attendance System (EAS) Using Bluetooth.
39. Adewumi AO, Akinyelu AA. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management. 2017;8(2):937-953.
40. Chakravorti S, To T. A theory of credit cards. International Journal of Industrial Organization. 2007;25(3):583-595.

41. Zheng L, *et al*. A new credit card fraud detecting method based on behavior certificate. In: 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC); 2018. IEEE.
42. Dabbagh M, Sookhar M, Dafa N. The Evolution of Blockchain: A Bibliometric Study. 2019.
43. Sael I, Benabbou N. Detection of credit card fraud: State of art. International Journal of Computer Network and Information Security. 2018.
44. Molloy I, Li J, Li N. Dynamic virtual credit card numbers. In: International Conference on Financial Cryptography and Data Security; 2007. Springer.
45. Altman E. Synthesizing credit card transactions. In: Proceedings of the Second ACM International Conference on AI in Finance; 2021.
46. Dighe D, Patil S, Kokate S. Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA); 2018. IEEE.
47. Sinkey JF, Nash RC. Assessing the riskiness and profitability of credit-card banks. Journal of Financial Services Research. 1993;7(2):127-150.
48. Yaokumah W, Ntow-Danso G. Credit card fraud detection. 2020. Available from: http://www.researchgate.net/. [Accessed 2022].
49. Dashiell S. Credit card statistics in the United States in 2022. Available from: https://www.finder.com/credit-card-statistics.
50. Liu D, Lee JH. Preventing chargeback fraud with blockchain. The Korean Institute of Communication and Information Sciences. 2022.