Cyber Attacks on Credit Card Transactions: A Comprehensive Review

Farhat Lamia Barsha
Department of Computer Science, Tennessee Technological University
fbarsha42@tntech.edu

***Abstract*— Credit card transactions have emerged as a vital component of worldwide commercial activities, facilitating smooth and efficient financial transactions. Nevertheless, the ease and convenience of credit card transactions have been accompanied by a corresponding drawback. Cybercriminals have persistently directed their efforts toward exploiting these transactions, thereby presenting a substantial threat to individuals, businesses, and financial institutions. A cyber attack targeting credit card transactions refers to any form of attack that seeks to illegally acquire or breach credit card data. The occurrence of cyber attacks targeting credit card transactions can result in severe consequences for both businesses and individuals, comprising financial damage, identity theft, and a negative impact on credit scores. Various types of attacks can be observed, which include skimming, phishing, malware, etc. The incidence of such attacks occurs in both digital transactions conducted online and through the physical act of card swiping. Efforts are being made to design systems that aim to safeguard novice users from such forms of cyber attacks. This article provides a brief review of the latest advancements in the detection of cyber attacks in credit card transactions. This brief study explores the primary approaches employed in detecting cyber crimes and then addresses the ongoing research challenges in the realm of cyber attacks on credit card transactions. The paper presents a concise overview of the research gaps identified and outlines potential future research areas. The findings of this analysis can be beneficial to other researchers working in this field, as it provides insights into the current state of threats on financial transactions.**

***Keywords*—Cyber attacks, Credit card fraud, Financial transactions, Cyber Security, Fraud detection, Machine learning.**

I. Introduction

Credit card fraud is an expression of identity theft that happens when an individual obtains someone's private information without authorization and uses it for financial transactions. The utilization of credit cards has recently experienced a significant rise due to the rapid growth of online transactions. As credit card utilization continues to increase, so does the risk of fraudulent activity, which can result in substantial financial losses for individuals and institutions [1]. According to the Nilson Report's December 2022 findings, it is projected that global losses resulting from card fraud will amount to $397.4 billion within the upcoming decade. Notably, the United States is anticipated to account for $165.1 billion of these losses [2]. The United States experienced a 13% rise in credit card fraud cases from 2021 to 2022 as shown in Figure 1.

Cyber attacks on credit card transactions are increasing worldwide. One of the most significant instances of cybercrime within the credit card system occurred in July 2019, specifically targeting the database of Capital One Bank [3]. A total of 106 million accounts had their information compromised, with 100 million originating from the United States and the remaining accounts belonging to Canadian users. According to [4], Capital One incurred financial penalties amounting to $80 million as a consequence of the data breach, which was facilitated by the misconfiguration of firewalls. Additionally, the company resolved consumer claims by paying a settlement of $190 million. Another incident took place in January 2009 on The Heartland company payment system. A total of 160 million credit card records, including personal identification information, were illegally acquired, resulting in an estimated financial loss of approximately $140 million [5]. The financial losses associated with credit and debit cards are growing steadily on an annual basis, thereby increasing the risk of a global financial disaster.

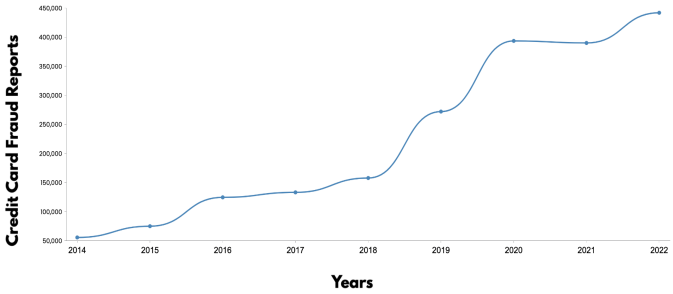

Fig. 1: Credit card fraud in the United States by year [6]

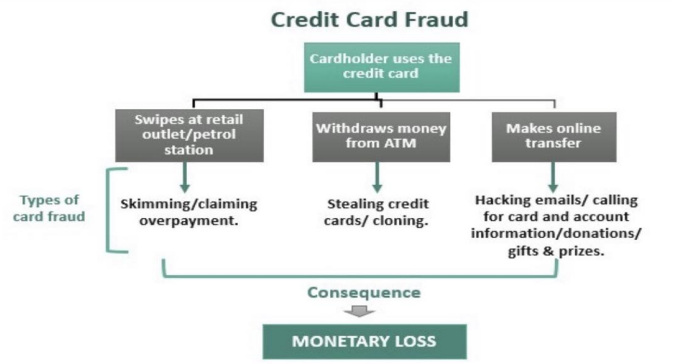

Fig. 2: credit card Fraud categories

Cyber attacks have the potential to occur during credit card transactions, whether they are conducted through physical card swiping or online platforms. In physical card swiping, cybercriminals can illegally copy card holders' personal data from the magnetic stripe of a credit or debit card through a skimming device installed on card readers like ATM, gas stations pumps etc. In case of online cyber attack, attackers possess the capability to hack email accounts, engage in the propagation of fraudulent electronic communications, and ask for sensitive card-related information. Figure 2 represents different forms of cyber attacks on credit card transactions.

There are different forms of cyber attacks such as phishing, skimming, data breaches, malware etc. Phishing attacks are a form of cybercriminal activity wherein attackers send fraudulent emails or text messages that replicate the appearance of authentic communications originating from trustworthy entities, such as financial institutions or credit card companies [7]. The electronic communications, such as emails or text messages, may potentially include a hyperlink directing users to a fraudulent website designed to resemble the authentic website. When a user submits their credit card information on the fraudulent website, the attackers illegally access the data . A skimming attack takes place when attackers attach a device onto a credit card reader with the purpose of secretly acquiring the magnetic stripe data of the card during the act of swiping. Card skimming refers to a form of cybercrime that involves the unauthorized acquisition of sensitive payment data by means of deploying malicious software, commonly referred to as a card skimmer, on an e-commerce platform [8]. The aforementioned data may be utilized for the purpose of producing fake credit cards or engaging in fraudulent online transactions.

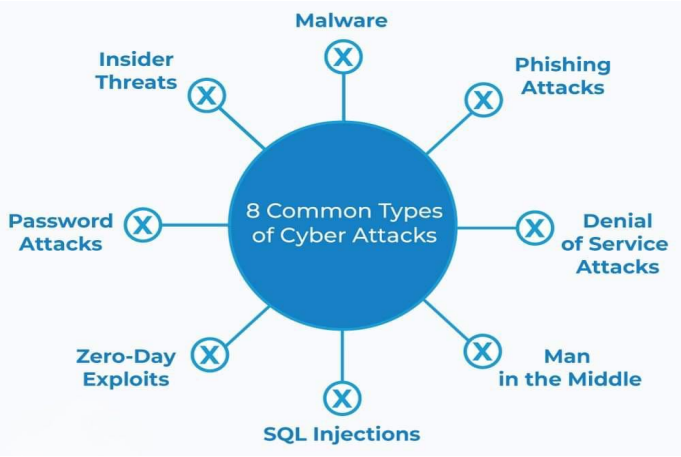

Fig. 3: Types of cyber security threats

A data breach involving credit card transactions refers to the illegal acquisition of sensitive credit card information, including card numbers, expiration dates, and CVV codes [9]. Subsequently, the acquired data can be exploited for fraudulent purposes, such as engaging in unauthorized transactions or initiating the establishment of new accounts under the identity of the targeted individual. Based on the findings reported by Statista, it was observed that a total of 1,473 data breaches occurred inside the United States throughout the year 2019 compromising of about 165 million personal data records [10]. Malware targeting credit card transactions refers to a form of malicious software designed with the intent to illicitly acquire credit card data [7]. The installation of malware on computers or mobile devices can occur silently and without the explicit approval or awareness of the user. Subsequently, this malware can be utilized to illicitly gather credit card information from websites, online businesses, and various other online transactions. Figure 3 represents 8 commonly occurring cyber security threats.

The effective management of cybercrime in credit card transactions is of utmost significance, as it serves to protect both individuals and the global economy. Cybercriminals frequently utilize complicated strategies that undergo fast evolution, necessitating a constant need to modify and enhance cybersecurity protocols [11]. Effectively mitigating cybercrime within this particular context not only serves to protect financial stability but also safeguards the privacy and financial security of numerous individuals, thereby reinforcing trust in the digital financial ecosystem.

The key contributions of this work are as follows:

1) An overview of the current state of research on security threats in credit card transactions, providing an overview of the existing literature.
2) An analysis of challenges associated with existing solutions for resolving the security issue of credit card transactions.

Recent IEEE, Elsevier, Springer, SCI, and Scopus-indexed research articles are reviewed in this work. About 70 Google Scholar research papers from top publishers were examined. After filtering the papers by keywords like cyber attacks, credit card fraud, cyber security etc., 10 papers were selected that mostly met the research work's requirements. Table I and Table II summarizes the research findings and gaps/possible future research in each literature.

We organize the rest of the paper as follows: In section II, I provided a comprehensive overview of the existing research conducted by current scholars. In Section III, the problem statement on cyber attacks on credit card transactions was formulated. I conclude the paper in section IV.

II. Research Overview

This section provides a concise overview of the literature pertaining to cyber attacks targeting financial transactions, namely those involving credit cards, debit cards, and internet transactions. The section is structured into three distinct components. The first part entails the categorization of the research problem. The second part involves a comprehensive discussion on the motivation for this work. Lastly, the third part offers a concise analysis of relevant literature.

Categorization/Tree Diagram of the research problems and solution methodologies: Figure 4 displays a tree diagram illustrating different aspects of credit cards and

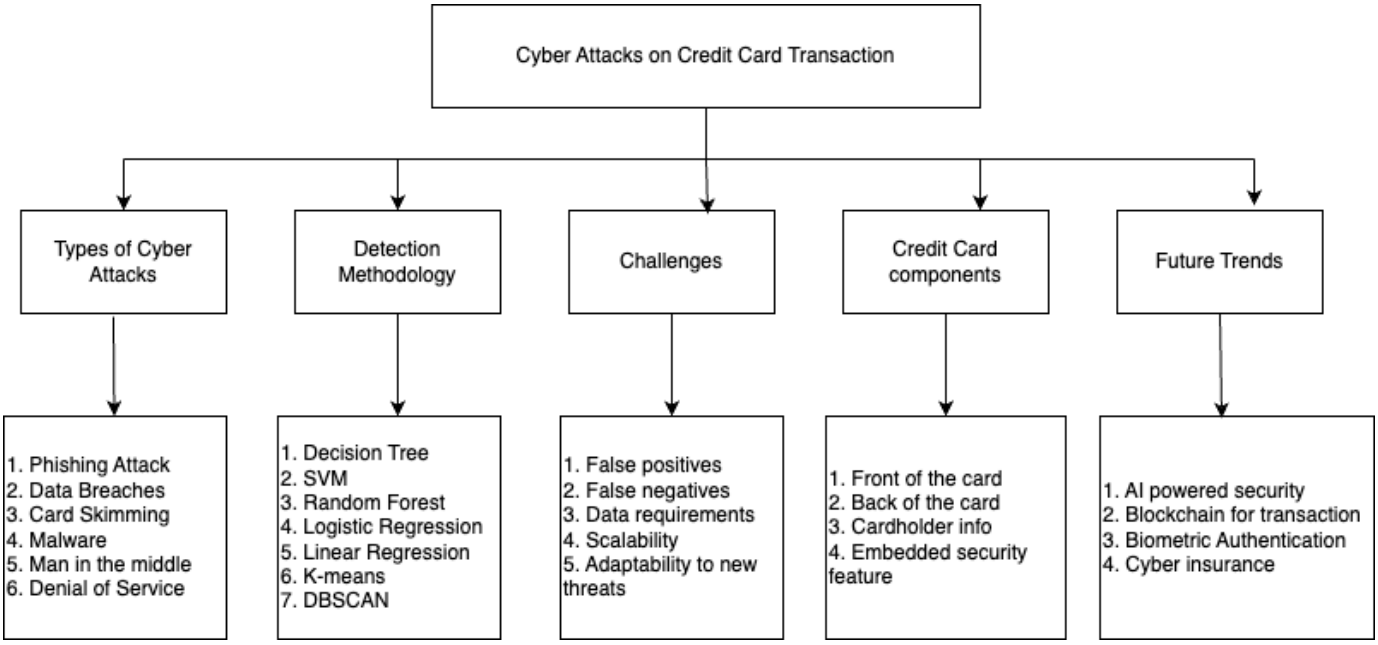

Fig. 4: Tree Diagram of the different aspects of Cyber Attacks on Credit Card Transactions

the methodologies employed to identify and mitigate cyber-attacks. The tree diagram includes five subsections pertaining to cyber attacks on credit card transactions, namely: Types of cyber attacks, cyber attack detection methodology, vulnerabilities, credit card components, and future trends.

Motivation and Rationale of the Research Problems/Solution Methodology tackled within each category: The motivation for studying cyber attacks on credit card transactions arises from the necessity to protect the financial security and privacy of individuals and organizations in an increasingly digital and interconnected world. Cybercriminals persistently employ advanced methods to exploit weaknesses in payment systems, resulting in financial losses, identity theft, and harm to one's reputation. It is imperative for financial institutions, businesses, and consumers to be aware of the aforementioned threats and vulnerabilities, as well as discern effective countermeasures. It is essential to develop techniques in order to reduce the risks associated with credit card fraud, safeguard sensitive financial information, and guarantee the security and reliability of electronic transactions. Researching malware attacks on credit card transactions can help us learn more about how these attacks work and how they can be stopped. This research aims to stay ahead of evolving cyber threats, enhance security measures, and maintain the trust and integrity of electronic payment systems. My doctoral research is focused on credit card fraud detection and I am working on integrating some new ideas into fraud detection techniques to develop a better detection approach.

Brief Summary of each paper in each category: Table I and Table II show important information by outlining the main/key research results, strengths, and weaknesses of each of the research papers/articles. In the next few lines, a short introduction will be added to each of the 10 papers that were chosen.

In [12], The authors have proposed a novel method wherein a notification message is sent to the cardholder prior to the one-time password (OTP) being generated. This notification is triggered anytime the customer or a potential hacker attempts to enter the credit or debit card number for an online transaction. In [5], The authors have put forth a proposal for a secure methodology that integrates the one-time credit card approach with machine learning algorithms. This approach demonstrates a high level of resilience against various potential cyber-attacks, unauthorized users, man-in-the-middle attacks, and guessing attacks related to credit card number generation or illegal financial activities. In [13], By examining a real transaction data set from the point of view of order, they find a new fraudulent transaction pattern called Replay Attack. Additionally, they have introduced a novel approach called the Replay Attack Killer (RAK) to identify and prevent instances of the Replay Attack. In [14], This study presents a proposed cybersecurity solution model aimed at safeguarding end users from a range of cyber threats, including phishing, malware detection, and ransomware detection. The framework offers a comprehensive solution for executing transactions, guaranteeing the secure transfer of shared information to external websites. In [15], the authors discussed the issue of credit and debit card fraud and examined the potential efficacy of employing multiple-factor authentication as a security technique to mitigate this criminal activity. The researchers put out the suggestion of including fingerprint recognition as an additional authentication factor.

TABLE I: Summary of the selected research papers for reviews on cyber attacks in credit card transactions

Reference paper	Summary of Core Idea	Point of Strength	Point of Weakness
Secure Credit or Debit Card Transaction Using Alert messages and OTP to prevent phishing attacks [12]	The suggested model is a simple way to protect Credit or Debit Cards in online transactions from phishing attacks. The proposed model prevent unauthorized transaction by sending an alert message to the customer when the hacker is using the Credit or Debit Card. They used the LUHN algorithm to validate the card number by the card issuing authority and send an alert message to the customer before generating OTP, if the transaction is unauthorized customer can block the card immediately. Otherwise system will proceed and generate OTP which will be used for a successful transaction.	Customer transaction messages are usually sent after the transaction. If the hacker knows the customer's credit or debit card data and has access to their email, they can complete a transaction using the OTP. The suggested model stops this kind of transaction by sending an alert message to the customer when a hacker is using their Credit or Debit Card. If the customer is unaware of this transaction, they can call the bank to block the card immediately before the successful occurrence of that transaction.	Generating an alert before each transaction is a bit hassle for customers, maintaining some thresholds can be a good option like if the transaction is above 1000 alert will be generated. As a future research direction, they proposed to generate biometric-based OTP which can ensure more security in transactions. Proper validation of the outcome of their proposed model is missing.
Secure and Fraud Proof Online Payment System for Credit Cards [5]	The system exhibits a high degree of resilience against various forms of cyber-attacks, unauthorized access attempts, man-in-the-middle attacks, and guessing attacks. The proposed system uses three security dimensions (one-time credit card number, secure communication medium, integrated with ML fraud detection algorithm) to ensure high security for every online credit card transaction. The generation of the distinct single-use credit card number is determined upon three elements, namely the time of the transaction, the amount of the transaction, and a randomly generated number.	This study presents a proposed method for generating a unique and verifiable one-time credit card number as a means of effectively mitigating the risks associated with database breaches. Additionally, a credit card fraud prevention system is proposed, incorporating multiple layers of security through the integration of authentication, machine learning-based fraud detection, and the generation of one-time credit card numbers.	The proposed approach causes a little overhead on the customer by requesting a one-time credit card number every time before proceeding to the regular process of making an online transaction.
Replay Attack: A Prevalent Pattern of Fraudulent Online Transactions [13]	This study examines a dataset of real B2C electronic transactions obtained from an Asian bank. The focus of the analysis is on the transaction sequence, leading to the identification of a common pattern associated with fraudulent transactions referred to as relay attack and also proposed the Replay Attack Killer (RAK), a novel method to detect and intercept the transactions that have the typical features of Replay Attack.	The majority of fraudulent transactions exhibit characteristics of rapid repetition, involving the same consumer and vendor, with transaction amounts that are closely aligned. This particular pattern is referred to as a Replay Attack. The presence of Replay Attack is demonstrated through rigorous statistical analysis, and a new fraud transaction detection system called Replay Attack Killer (RAK) is introduced. Through experimentation, it has been demonstrated that the RAK system is capable of effectively identifying and flagging up to 92% of fraudulent transactions in real-time while causing minimal disruption to only 0.06% of legitimate transactions.	The replication of relay attacks in future data, across different banks and time periods, is not feasible due to the dynamic nature of fraud. Fraud is a rapidly evolving phenomenon that adapts to market conditions and the countermeasures implemented by financial institutions. Future plan is to try B2C fraud detection approaches to see whether they work better with RAK and vice versa, apply RAK into computing clusters to test the speed improvement in real bank environments, and examine the data set more.
Protecting Online Transactions: A Cybersecurity Solution Model [14]	The present study presents a conceptual framework for a cybersecurity solution model aimed at safeguarding online transactions and mitigating the potential hazards associated with cyberattacks. The model emphasizes the significance of employing OTP verification and password protection as security measures to safeguard transactions. The framwork utilizes deep-learning CNNs to train the model.	The primary contribution of this research study lies in the formulation of a security solutions model that integrates hybrid methodologies, machine learning algorithms, and biometric recognition techniques to safeguard data against potential cyber threats. This is achieved by the implementation of access restrictions and the facilitation of content sharing in accordance with user permissions, accomplished by establishing user interactions that adhere to specified criteria for requirements and information resources. The model can identify 95% malware, 96% phishing, and 98% ransomware attacks.	Online transactions data on third-party websites is used to train the model but not enough information is available regarding the dataset.
Multiple Factor Authentication as a Security Measure in Credit Card Fraud [15]	This paper aims to strengthen credit card security to make the context to be adopted by everyone even those who lack developed techniques by using simple techniques like fingerprint as a multiple authentication. They used three-factor authentication and used fingerprint as a third authentication method.	Multiple authentications are the fact of combining more than two methods of authentication with the aim of strengthening the security level. They compared three-factor authentication with one or two-factor authentication and found that by using three-factor authentication even with a basic authentication method like a fingerprint, the security is high, complexity is strong and the vulnerability is low.	Future research will focus on enhancing the security of the final step authentication procedure to prevent any potential compromises. It is imperative to prioritize the selection of the third authentication factor by carefully assessing its user-friendliness while avoiding unnecessary complexity. They should also consider cost, compatibility, maintenance, and privacy.

TABLE II: Summary of the selected research papers for reviews on cyber attacks in credit card transactions

Reference paper	Summary of Core Idea	Point of Strength	Point of Weakness
An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies [16]	This study aims to evaluate the effectiveness of a three-factor authentication strategy that incorporates Near Field Communication (NFC), the Dash Matrix Algorithm, and One-time password (OTP). The objective is to assess the capability of this scheme in mitigating common transaction vulnerabilities such as brute force attacks, shoulder surfing, and skimming of ATM cards. The implementation of the supplementary functionality for preventing ATM cards involves the utilization of a QR code authentication system and NFC technology. This implementation is applicable to both NFC-enabled smartphones and non-NFC smartphones.	The suggested system aims to provide secure utilization of ATM cards while also being cost-effective through the implementation of innovative and widely adopted technology. Additionally, the system is designed to be user-friendly. Development of this model includes Secured ATM transactions using NFC, Blocking of lost ATM cards, NFC Registration, and facilitation of NFC using non-NFC mobile phones.	One potential avenue for future improvement involves the utilization of the NTag21x family of tags. This particular family represents a recent technological innovation characterized by enhanced security measures and improved read capacity. Additionally, the utilization of MIFARE DESFire EV2 and MIFARE SAM AV2 cards is possible due to their provision of AES encryption and secure storage capabilities for cryptographic keys. The tags may be evaluated for compatibility with NFC-enabled smartphones, whereas the latter can be utilized with mobile devices that do not support NFC technology.
A Secure Credit Card Protocol over NFC [17]	In this paper, the authors identified prevalent attacks on the NFC credit card protocol and designed an alternative credit card protocol that defends against all of these attacks. They used stepwise refinement to construct this secure protocol and prove its correctness in the face of these attacks. The protocol exclusively employs cost-effective primitives such as pre-computed hashes, indexing, and XOR operations, while maintaining a demonstrable level of security against the specified attacks. The protocol also ensures that retailers maintain their ability to correlate purchases from the same credit card.	Changing operational systems, especially in the payment business, is difficult. Thus, they provide a way to apply their protocol without modifying payment processing systems. By installing a ”payment proxy,” the bank can translate charge requests from their secure protocol to the existing protocol. Banks can support Points-of-Sale that use the susceptible protocol by not changing the present systems. They do so to ease acceptance in an industry that resists change.	The authors examine four prevalent attacks that exploit existing weaknesses in NFC technology. However, they do not explicitly address whether their proposed model is capable of defending against other potential attacks.
Analysis of Credit Card Attacks Using the NFC Technology [18]	This study presents an analysis of the current state-of-the-art in Near Field Communication (NFC) technology as applied to payment systems. The objective was to evaluate existing research and effectively execute attacks in order to assess the potential risks that this technology may offer to end-users. The authors contend that NFC systems employed in financial transactions yield insufficient financial benefits, particularly when considering the limited unauthorized transaction threshold, in contrast to the considerable time and effort involved in stealing funds from NFC-enabled cards, organizing a malicious point-of-sale system to execute the transactions, and related activities.	In this study, the authors mostly talked about relay attacks. They also looked at unauthorized card reading and talked about eavesdropping, data manipulation, and man-in-the-middle attacks. After looking at how secure NFC technology is in different ways, they came to the conclusion that mobile payments have a lot of benefits that make up for the few security problems they have.	The main constraint of the research that examines NFC technology for payment security is its probable deficiency in comprehensiveness, as it concentrates on a small range of attacks and vulnerabilities. The possibility exists for an inadequate evaluation of the continuously developing NFC security environment, neglecting emerging risks and disregarding various contextual elements, user actions, and legal factors that can substantially influence the overall level of risk associated with NFC technology in payment systems.
A Three-Level Gateway Protocol for secure MCommerce Transactions using Encrypted OTP [19]	This paper introduces a protocol called the Three-Level Gateway Protocol for Secure M-Commerce Deals. The protocol utilizes a conventional or public-key algorithm, as well as the Advanced Message Queuing Protocol (AMQP), which is an open standard for exchanging messages between operations or associations. Additionally, an Encrypted OTP is employed in the payment process to guarantee the confidentiality of data and to safeguard against Replay Attacks, Man in the Middle Attacks, and Masking attacks on Cryptography systems.	Several security issues were addressed in the present essay. One of the most effective approaches for ensuring the security of encrypting and decrypting One-Time Passwords (OTPs) is to utilize conventional or public/private key encryption techniques, which are widely accessible. The selection of key size, data size, and devices for algorithm implementation is influenced by various advantages and disadvantages associated with each factor.	One of their major limitations is they didn't compare their proposed model with any alternative payment methods to validate the result. As future research they propose to conduct simulations of the proposed Three Level Gateway Protocol for Secure M-Commerce Transactions and doing a comparative analysis with alternative payment methods that employ conventional encryption techniques and public key/private key cryptosystems, all within the framework of the AMQP protocol. Another factor is that the protocol should be customized to suit different contextual requirements.
Role of multiple encryption in secure electronic transaction [20]	This research study proposes the incorporation of numerous encryption techniques in Secure Electronic Transactions (SET) to augment the security measures employed for safeguarding personal data. Multiple encryption in Secure Electronic Transaction provides better security and ensures confidentiality and privacy of original data.	This concept presents a divergence from the current data encryption technique employed in Secure Electronic Transaction standards, aiming to enhance information security in wireless networks such as the Internet. The utilization of several layers of data encryption, employing advanced encryption keys, has the potential to significantly bolster data security.	The encryption and decryption processes are more complicated, resulting in a substantial rise in complexity. Consequently, a considerable amount of time is necessary to study and determine the correct keys for decrypting the encrypted data.

In [16], The authors present a proposed system that utilizes a three-factor authentication strategy incorporating Near Field Communication (NFC), Dash Matrix Algorithm, and One-time password. They proceed to discuss and assess the system's potential to mitigate various transaction vulnerabilities, such as brute force attacks, shoulder surfing, and skimming of ATM cards. In [17], The authors use stepwise improvement to make a secure NFC credit card protocol using only inexpensive primitives such as pre-computed hashes, indexing, and XOR operations. the protocol protects against eavesdropping, skimming, relay attacks, and compromised Points-of-Sale. In [18], The authors conduct an analysis of the current state-of-the-art in Near Field Communication (NFC) technology. In [19], the authors introduce a Three-Level Gateway Protocol for Secure M-Commerce Deals, utilizing any conventional or public-critical algorithm, AMQP, an open standard for message passing, and an Encrypted OTP for payment confidentiality and prevention of Replay, Man in the Middle, and Masking attacks on cryptography systems. In [20], the need of multiple encryption techniques in Secure Electronic Transaction are proposed to enhance the security of confidential data.

III. Research Problem

Cybersecurity breaches targeting credit cards encompass a range of strategies, encompassing card-not-present fraud during online transactions, as well as identity theft when perpetrators exploit personal data to carry out unlawful activities. These occurrences emphasize the significance for implementing effective cybersecurity protocols and developing a state of constant awareness among credit card holders. The existing research has numerous limitations, hence presenting potential avenues for future research endeavors. I am interested in choosing one significant aspect of the issue in detecting cyber threats to focus on for my term project.

Selection of Problems from the choice of categories: The credit card transaction domain presents numerous obstacles in the realm of cyber attack detection techniques, as depicted in Figure 4. One of the primary challenges is the occurrence of false positives, which entails several adverse outcomes for both businesses and consumers. These implications encompass financial losses, customer unhappiness, operational burdens, and security vulnerabilities. My primary goal will be to address the problem of false positive occurrences. Addressing the issue of false positive identifications in credit card fraud detection involves a continuous process necessitating the integration of technology progressions, accurate data analysis, and a constant dedication to balancing security measures with customer convenience.

Definition of the Problems: Within the realm of credit card transaction cyber attack detection, the matter of false positives arises when genuine transactions or activity are erroneously classified as potential instances of fraud or cyber assaults. This issue presents several difficulties, such as inconveniencing users, causing delays in transactions, resulting in declined transactions, diminishing trust, increasing operational burdens, and raising the possibility of missing real threats. Achieving an optimal equilibrium between effective fraud detection measures and the mitigation of false alarms is crucial in safeguarding the integrity of credit card transactions, while concurrently upholding a satisfactory user experience and fostering confidence between cardholders and financial institutions. The implementation of ongoing enhancements in fraud detection models and technologies, along with the integration of user education and feedback mechanisms, play a crucial role in effectively resolving and minimizing the consequences of false positives within this vital field.

Motivations for working on this problem: There are many reasons to try to cut down on false positives in cybersecurity and fraud detection. First of all, false positives can make users frustrated and cause them trouble, which hurts the user experience. Second, they can cause delays in transactions and cause valid transactions to be turned down, which can cause businesses to lose money. Third, false positives can put a strain on management resources because it takes more time and people to look into and deal with alerts. Fourth, too many false positives can make people lose faith in security systems, which could cause them to stop using services. Lastly, lowering false positives is important for allocating cybersecurity resources efficiently and making sure that real security threats are quickly found and dealt with.

Summary of limitations of research in the selected category: In the chosen subject of study, there is a limited quantity of articles that have been selected inside this particular research category for further investigation. Given the limited number of scholarly articles addressing the false positive issue and its associated implications, there exists a significant opportunity for further investigation and research in this domain. A significant proportion of the studies fail to incorporate false positives as a parameter for assessing the efficacy of their proposed model.

Proposal of Solution Methodology and Expected Challenges + Possible Contributions: Based on the review of the literature, I have chosen some key research gaps to work on in order to move the project forward. To deal with false positives in cyber attack detection, I want to use advanced machine learning techniques, like anomaly detection, that can adapt to changing attack trends and constantly learn from new data to reduce false positives while keeping a high level of detection accuracy.

The initial step involves selecting a dataset of legitimate transactions, which will serve as the foundation for creating a baseline or profile of anticipated behavior for the purpose of anomaly identification. An additional dataset must be generated for the purpose of analysis, wherein transaction attributes such as money, location, time, and user behavior are carefully selected and engineered. In the subsequent step, I intend to select an anomaly detection model, such as Isolation Forests or One-Class SVM, and proceed to train it using a dataset consisting of normal behavioral patterns. A crucial aspect of anomaly detection involves

the establishment of a suitable threshold, which serves to define the extent of deviation from the established norm that warrants the activation of an alert. The deployed model must be operationalized within a real-time monitoring setting, whereby it consistently assesses incoming transactions or events. When a transaction or behavior is identified as deviating significantly from the established norm and over the predetermined threshold, an alert will be generated. This warning serves as an indication of possible anomalous or suspicious conduct. Notifications are dispatched to cybersecurity analysts or automated systems for the purpose of examination and subsequent inquiry. Analysts evaluate the generated alerts in order to ascertain their validity as potential threats or ascertain whether they are false positives. This technique will enhance the precision and effectiveness of fraud and intrusion detection systems by emphasizing the identification of unusual patterns and deviations from the established norm, hence reducing the occurrence of false warnings and disruptions.

IV. Conclusion

The occurrence of cyber attacks targeting credit card fraud is an ongoing and dynamic concern within today's digital landscape. The imperative to tackle this matter is of utmost importance, requiring ongoing investigation, advancement, and cooperation among financial institutions, cybersecurity specialists, and technology vendors. Ongoing efforts are being made to address persistent issues in the realm of credit card transactions, including false positives, data imbalances, and fast-evolving attack strategies. These endeavors are aimed at mitigating risks and upholding the trustworthiness and integrity of electronic payments.

This paper presents a concise overview of various forms of cyber attacks targeting credit cards, as well as the current techniques proposed by researchers to effectively mitigate these attacks. The present study reveals that the issue of false positives poses a significant obstacle in the realm of cyber attack detection approaches. Addressing this challenge in a timely manner is crucial for enhancing the efficacy of detection methods and reducing the occurrence of false alerts. In an interconnected and digital world, the implementation of cybersecurity measures, user education, and regulatory compliance are crucial elements of a comprehensive strategy aimed at mitigating cyber attacks pertaining to credit card fraud.

References

[1] A. H. Alhazmi and N. Aljehane, "A survey of credit card fraud detection use machine learning," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*. IEEE, 2020, pp. 1–6.

[2] J. Egan, "Credit Card Fraud Statistics — Bankrate — bankrate.com," https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics/, 2023.

[3] "2019 Capital One Cyber Incident — What Happened — Capital One — capitalone.com," https://www.capitalone.com/digital/facts2019/, [Accessed 27-09-2023].

[4] "Paige Thompson found guilty in 2019 Capital One data breach — TechTarget — techtarget.com," https://www.techtarget.com/searchsecurity/news/252521775/Paige-Thompson-found-guilty-in-2019-Capital-One-data-breach#:~:text=As%20a%20result%20of%20the,for%20fraud%2C%20analysis%20proved%20difficult., [Accessed 27-09-2023].

[5] B. Al Smadi, A. A. S. AlQahtani, and H. Alamleh, "Secure and fraud proof online payment system for credit cards," in *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2021, pp. 0264–0268.

[6] "Consumer sentinel network," https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf.

[7] "How Do Hackers Steal Credit Card Information? — TechTarget — techtarget.com," https://www.techtarget.com/whatis/feature/How-do-cybercriminals-steal-credit-card-information, [Accessed 27-09-2023].

[8] K. Sheldon, "Card Skimming: What It Is and How to Prevent It — ithemes.com," https://ithemes.com/blog/card-skimming-what-it-is-and-how-to-prevent-it/, [Accessed 27-09-2023].

[9] "Credit Card Data Breach: What It Is amp; Ways To Prevent It — Chase — chase.com," https://www.chase.com/personal/credit-cards/education/basics/credit-card-data-breach, [Accessed 27-09-2023].

[10] "Data Breach Statistics to Know for 2023 — Rivial Security — rivialsecurity.com," https://www.rivialsecurity.com/blog/data-breach-statistics#:~:text=There%20were%201%2C473%20Data%20Breaches,164.68%20million%20sensitive%20records%20exposed.%E2%80%9D, [Accessed 27-09-2023].

[11] "Understanding the Threat of Card Transaction Fraud and its Impact on the Financial Ecosystem — Waylay Blog — waylay.io," https://shorturl.at/yCHO4, [Accessed 27-09-2023].

[12] S. Kumari, K. Kumar, G. Gupta, P. Rajakumar *et al.*, "Secure credit or debit card transaction using alert messages and otp to prevent phishing attacks," in *2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM)*. IEEE, 2023, pp. 1–5.

[13] C. Jing, C. Wang, and C. Yan, "Replay attack: A prevalent pattern of fraudulent online transactions," in *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2018, pp. 75–82.

[14] S. Surya, S. R. Jagtap, R. Ramnarayan, M. Priyadarshini, R. K. Ibrahim, and M. B. Alazzam, "Protecting online transactions: A cybersecurity solution model," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2023, pp. 2630–2634.

[15] G. O. Boussi and H. Gupta, "Multiple factor authentication as a security measure in credit card fraud," in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2020, pp. 94–98.

[16] A. Mandalapu, D. Deepa, L. D. Raj *et al.*, "An nfc featured three level authentication system for tenable transaction and abridgment of atm card blocking intricacies," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*. IEEE, 2015, pp. 1–6.

[17] O. Jensen, M. Gouda, and L. Qiu, "A secure credit card protocol over nfc," in *Proceedings of the 17th international conference on distributed computing and networking*, 2016, pp. 1–9.

[18] J. Jumić and M. Vuković, "Analysis of credit card attacks using the nfc technology," in *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2017, pp. 1251–1255.

[19] S. Ramana, S. C. Ramu, N. Bhaskar, M. R. Murthy, and C. Reddy, "A three-level gateway protocol for secure m-commerce transactions using encrypted otp," in *2022 International conference on applied artificial intelligence and computing (ICAAIC)*. IEEE, 2022, pp. 1408–1416.

[20] H. Gupta and V. K. Sharma, "Role of multiple encryption in secure electronic transaction," *International Journal of Network Security & Its Applications*, vol. 3, no. 6, p. 89, 2011.