International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Online Payment Fraud Cause and Prevention Technique

Suraj Charde, Kashish Kayate

G H Raisoni University, Amravati, Maharashtra, India

Abstract

Online fraudulent transactions are a significant criminal violation. Every it costs people and financial institutions billions of dollars. It emphasizes the crucial importance of financial institutions in detecting and preventing fraudulent acts. Machine learning algorithms provide a proactive way mechanism to prevent online transaction frauds with high accuracy. Online transaction fraud is a simple and easy target. E-commerce and other online sites have increased the number of online payment methods, raising the danger of online fraud. With the rise in fraud rates, machine learning approaches can be used to identify and evaluate fraud in online transactions. The primary goal of this project is to implement supervised machine learning models for fraud detection, with the goal of analyzing prior transaction information. Where transactions are classified into distinct groups based on the type of transaction. Following that, various classifiers are trained independently, and models are assessed for correctness. The classifier with the highest rating score can then be picked as one of the best approaches for predicting fraud. We worked with the Kaggle Synthetic Financial Datasets for Fraud Detection dataset collected by Edgar Lopez-Rojas. The use of technology and online shopping has gone up a lot and so has the use of online payment systems like credit cards, debit cards, mobile wallets and internet banking.

This has given cybercriminals a chance to do things. People, businesses, and financial institutions think that payment fraud is a big problem. Things like phishing attacks, identity theft, fake websites and malware attacks cause people to lose money. In this research paper we will talk about why online payment fraud happens and look at kinds of online payment fraud. One big reason for payment fraud is that people who use the internet do not know enough about how to keep themselves safe from cyber-attacks like phishing emails and suspicious links. Also not having enough security measures like passwords and networks makes it easy for cybercriminals to commit online payment fraud. The fact that we can now do things on our phones and online has made it even easier for cybercriminals to commit payment fraud. This has been a worry for people who use the internet for a long time. This paper will also talk about some ways to stop payment fraud like using multi-factor authentication secure encryption techniques, tokenization, biometric authentication, and detection systems that use machine learning algorithms. Online payment fraud is a problem and online payment fraud can be stopped with the help of machine learning models that can look at transactions in real time and find anything suspicious. This way banks and other financial institutions can stop transactions before they cause a lot of damage. It is also very important for people to learn about payment security and get updates on the latest threats. The study found out that we need to use a combination of technology and awareness to stop payment fraud. If financial institutions use the security systems, they can reduce the risk of fraud and make people trust online payment systems more. This research helps us understand why online payment fraud happens and how we can stop it which makes the internet a safer place for people to do their finances.

KEYWORDS*: Online Payment Fraud, Digital Payment Security, Cyber Fraud Detection, Phishing Attacks, Identity Theft, Machine Learning in Fraud Detection, Multi-Factor Authentication (MFA), Secure Electronic Transactions, Financial Cybersecurity, Fraud Prevention Techniques.*

1. INTRODUCTION

Over the few years digital technology has changed the way we do financial transactions. We can now use payment systems like internet banking, credit cards debit cards and digital payment applications to make transactions faster and easier. Many people use these systems to buy things pay bills and do transactions. With the growth of payments online payment fraud has also increased. Online payment fraud is when someone does a transaction on the internet to get money. Online cybercriminals use methods like phishing, identity theft and malware to trick people and get their information, including bank account numbers and passwords. This can cause losses for individuals, companies, and banks. As more people do transactions online cybercriminals are finding ways to exploit weaknesses in payment systems.

One of the reasons for payment fraud is that people do not know enough about cybersecurity. Many people unknowingly give away information by clicking on links, which lets the attacker access their financial account. Using passwords, unsecured networks and old software can also increase the risk of cyber-attacks. Sometimes attackers create websites or apps that look real. People give away their personal information. To reduce payment fraud, financial and technology companies are working on advanced security systems. They use encryption, secure authentication, fraud detection and machine learning to analyze patterns and detect activities in time. Machine learning is important for detecting activities and preventing transactions.

Technology is not enough. People need to be aware of practices like protecting their personal details checking if a website is legitimate and being careful when using public wireless networks. Governments and financial regulatory bodies are also making rules to safeguard payment systems. The main goal of this research paper is to look at the causes of payment fraud and discuss ways to prevent it. It also talks about how technology, like machine learning and authentication can be used to prevent payment fraud. We need to understand the causes of payment fraud and take steps to prevent it so we can have a safer online payment environment. Online payment fraud is a problem and online payment systems are the target. We need to be careful when

we use payment systems and take steps to protect ourselves from online payment fraud.

Online payment systems are convenient and easy to use. We need to be aware of the risks. Online payment fraud can happen to anyone, so we need to be careful and take steps to protect ourselves. We can use payment systems safely if we are aware of the risks and take steps to prevent online payment fraud. We need to understand this connection to prevent online payment fraud.

Fig1. Online payment fraud

2. Literature Review

The growth of payment systems and online business has caused online payment fraud risks to go up all over the world. Many people have done research to find out why financial fraud happens and to come up with ways to detect and stop online payment fraud. In this part we will talk about what other people have found out about payment fraud risks how to detect online payment fraud and how machine learning can help prevent financial crimes. Online payment fraud risks have gone up a lot because of the growth of payments. Online banking fraud is one of the risks in financial systems all over the world. This is when bad people get into financial accounts without permission and do illegal things with money. It is hard to find banking fraud because there are not many fake transactions compared to all the real ones and the patterns of fake activities are complicated.

Many people have studied how machine learning can help find payment fraud. Usually people use rule-based systems to detect payment fraud. This does not work well when there are a lot of online transactions. New machine learning models can look at a lot of data. Find unusual patterns in payment transactions. Models like Logistic Regression, Decision Trees, Random Forest Support Vector Machines and Neural Networks can all be used to detect financial transactions. We looked at what other people have written about using machine learning to detect fraud. We found that supervised learning is still used a lot because it is easy to understand and works well. Unsupervised learning and anomaly detection are also becoming more important for finding new and unseen patterns of financial fraud. Deep learning models like convolution networks and recurrent neural networks are also being used more to detect financial fraud especially for looking at complicated transaction behavior.

Another study found that using machine learning algorithms together can be very accurate in detecting fake activities. For example, Gradient Boosting and Random Forest algorithms worked well in detecting activities in e-commerce datasets. In one study the Gradient Boosting algorithm was able to predict activities with an accuracy of 99.7%, which is very good. Researchers also think that handling data is very important when making fraud detection systems. Financial data about fraud detection is often not balanced because there are not fake transactions compared to real ones. This makes the model not work well. Most studies have focused on ways to make the model work better like choosing the features resampling and anomaly detection. New studies are also using technologies like artificial intelligence and deep learning to make fraud detection better. For example, artificial intelligence systems can watch what users do look at transaction history, device data and where people are to find activities in real time.

Artificial intelligence systems can learn from data and adapt to new fake activities, which makes them better at detecting fake activities than traditional methods. Some studies have also suggested using a combination of approaches to make detecting activities more accurate. These models use algorithms and approaches to detect fake activities. They can detect fake activities, and this is recommended for modern financial security systems. In all online payment fraud is a big problem all over the world that is getting worse because of more online transactions. Most researchers agree that advanced technologies like machine learning, artificial intelligence and online monitoring systems are necessary to find and prevent transactions. Problems like

data imbalance, fraud techniques and accuracy, in online systems still need to be researched and developed. Online payment fraud and online payment fraud risks are still a concern and need to be addressed by using machine learning and artificial intelligence to detect and prevent online payment fraud.

Online payment fraud is a problem and people have been working on ways to stop it using technology. They have been using computer programs like Decision Trees and Neural Networks to look at information about payments and find anything that does not seem right. These programs are trained on a lot of data from payments to help them figure out what is normal and what is not. Many studies have shown that these programs can really help make online payment systems at finding fraud. A lot of people are also working on making systems that can watch payments in time to catch fraud as it happens and reduce the amount of money that is lost. Some studies have also talked about how important it is for people to be aware of online payment fraud and for companies to use strong security measures, like two-factor authentication to keep people safe.

Online payment fraud is something that we need to take, and we need to use technology and other security measures to stop it. We can use payment fraud detection systems and other methods to reduce online payment fraud. Online payment fraud detection systems are very important. We need to use them to reduce online payment fraud.

3. Research Methodology

Research methodology is defined as a systematic method used to collect and interpret data for a research study. It provides an explanation of how the research is conducted and helps to ensure that it is reliable and valid. The aim and objective of this research are to identify the major causes of online payment fraud and to study different techniques used to reduce the risk of fraudulent practices. This study has used a qualitative and analytical research approach. The qualitative research approach has been used to understand the nature of online payment fraud and the behavior of cybercriminals. The analytical research approach has been used to identify different techniques used to reduce the risk of fraudulent practices. This research has used a descriptive research design. Descriptive research helps to identify a detailed explanation of the causes of online payment fraud and different security measures used to reduce the risk of such practices. This research design has helped the researcher to describe different types of online payment fraud, such as phishing, identity theft, malware, and unauthorized transactions. The research is primarily based on secondary data collection. The meaning of secondary data collection is the information that has already been collected by other researchers, organizations, and institutions. The use of secondary data collection will help in understanding the research that has been conducted in the field of digital payment security.

The data that has been collected is analyzed through comparative analysis and content analysis techniques. The comparative analysis technique is used to compare the different fraud detection techniques to understand the advantages and disadvantages of the techniques that can be used to detect fraudulent transactions. The content analysis is done to understand the information available in different research papers and reports to identify common themes related to online payment fraud. This analysis is important in understanding the causes of fraud and how cybercriminals use different techniques to exploit online payment systems.The research is also focused on analyzing different modern technology solutions related to machine learning algorithms, artificial intelligence systems, and different online monitoring tools used to detect fraudulent activities in online transactions.

The scope of this research is focused on understanding the major causes of online payment fraud and identifying the most effective techniques for preventing fraud in modern online payment systems. The online payment fraud is mainly related to fraud in online banking systems, mobile payment applications, and online e-commerce platforms. The research also points out the importance of emerging technologies like artificial intelligence and machine learning in enhancing the quality of fraud detection systems. Although it can be said that the research has provided significant insights into online payment fraud and techniques used to prevent it, it has some limitations too. The research has primarily used secondary data sources to gather information. Therefore, it entirely depends upon the authenticity of secondary data sources. No primary research has been carried out through surveys or interviews with users or financial institutions.

Another significant aspect of this research methodology is the analysis of fraud detection and prevention techniques. Various techniques employed by banks and online payment systems to detect and prevent fraud have been analyzed and compared in this research methodology. The techniques analyzed in this research methodology include the use of secure payment gateways, two-factor verification, OTP verification, encryption technology, fraud detection systems, and machine learning algorithms. Machine learning algorithms are increasingly being used to detect abnormal transaction patterns and prevent fraudulent activities in real-time. By analyzing different fraud prevention techniques, the research identifies the effectiveness of different techniques in preventing online payment fraud.

Descriptive and analytical analysis is performed on the data collected in this research methodology. The data collected from different sources is analyzed, classified, and interpreted to identify important patterns and trends in online payment fraud. Descriptive analysis is performed to explain the causes and types of fraud, while analytical analysis is performed to explain the effectiveness of different fraud prevention techniques. Moreover, the research study also examines the role played by user awareness and cybersecurity education in preventing online frauds. It has been observed that online frauds take place due to inadequate awareness among internet users regarding online safety and security best practices. Therefore, it is important to educate internet users regarding online safety and security. It may be concluded that the research methodology adopted in the above study offers a systematic approach to understand the causes and prevention techniques of online payment frauds. The study has used secondary research data and case study research to compare different techniques used to detect online payment frauds and to develop a comprehensive knowledge regarding online payment frauds and how it can be minimized to avoid financial losses.

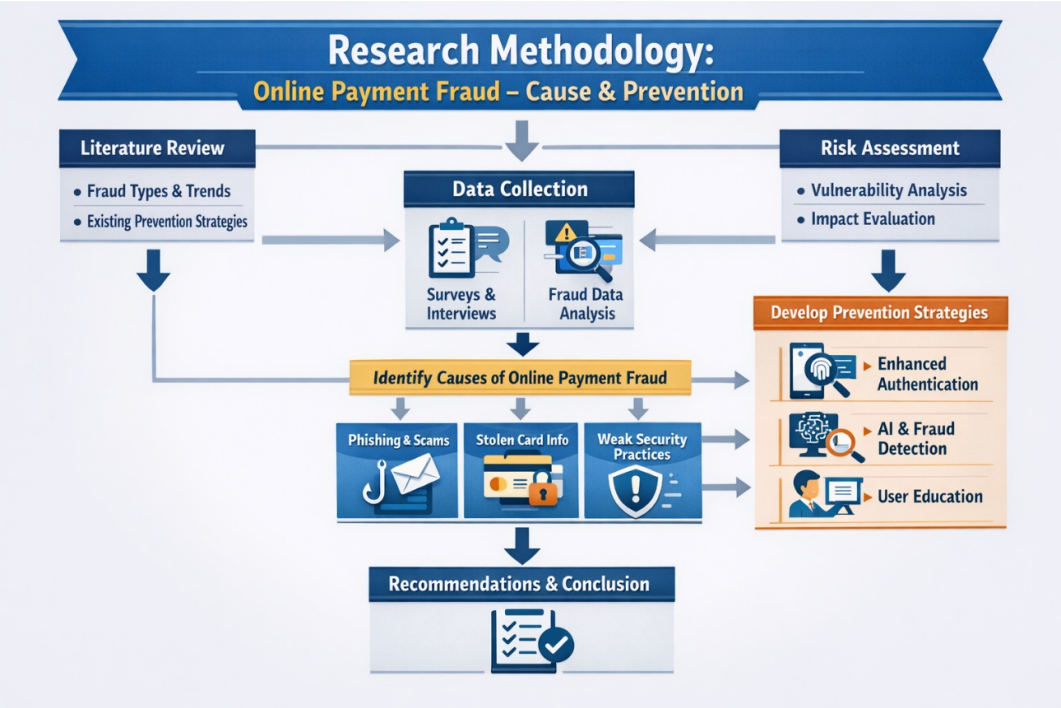

Fig 2. Proposed research methodology framework.

This diagram is about the research methodology for Online Payment Fraud: Causes and Prevention Techniques. It starts with looking at what other people have said about payment fraud. This means reading studies and reports to see what we already know about online payment fraud. The next step is to collect information from people who have been affected by online payment fraud. This is done by asking people questions and looking at cases where online payment fraud happened. The information that is collected is then looked at closely to find the reasons why online payment fraud happens. These reasons include things like phishing attacks and people using passwords.

After that the research looks at the risks of payment fraud. This means finding out where the weaknesses are in payment systems and how bad it could be if someone takes advantage of these weaknesses. The research then tries to find ways to stop payment fraud from happening. This includes using ways to check if someone is who they say they are like using a password and a special code sent to their phone. It also includes using computers to detect when someone is trying to commit online payment fraud.

Online Payment Fraud is a problem, and the research wants to help people understand how to protect themselves. So, it teaches people how to recognize when someone is trying to commit payment fraud and how to keep their money safe. Finally, the research gives ideas and conclusions to help banks, businesses and people make online payments safer and reduce Online Payment Fraud. The goal is to make Online Payment Fraud less of a problem, for everyone. This study is about payment systems, and it uses a qualitative and descriptive research approach. The qualitative approach clarifies the kinds of fraud that happen how users behave and what security problems exist in online payment systems. We use research to explain the patterns of fraud what causes it and how to prevent it.

The data for this study comes from sources. We got information from journals, research papers, government reports, banking websites, cybersecurity reports and other trusted online sources. These sources give us ideas about the different types of fraud like phishing, identity theft, fake websites and OTP scams. By looking at data we can see how online payment fraud is changing and growing on different digital platforms. This study also looks at how aware usersre how they practice cybersecurity to prevent online payment fraud. We look at things like using passwords sharing OTPs clicking on suspicious links and using networks that are not secure. We want to understand how the things users do can lead to fraud.

4. Result

The results of this study show that online payment fraud is a problem that is getting worse because more and more people are using online payment systems and e-commerce sites. When we looked at what other people have found out about this, we saw that there are reasons why online payment fraud is happening. One of the reasons for online payment fraud is that people do not know enough about how to keep themselves safe online. Often people do not even realize they are giving away information like their passwords or bank account information to bad people who are trying to trick them through emails or messages. Also using passwords and not having good security along with using public computers makes it easier for bad people to attack online users. The study also found that phishing, identity theft, websites, malware attacks and unauthorized transactions are some of the most common types of online payment system fraud. Bad people on the internet try to make websites or apps that look like real online payment sites so they can trick people and get their money information.

The study also found that technology is really helping to stop payment fraud. Banks and other financial institutions are using technologies to stop bad people from getting away with fraud. For example, they are using machine learning and artificial intelligence to look at lots of information and find patterns that might mean someone is trying to commit fraud. They are also watching transactions in time to catch fraud and stop people from losing money. Additionally

making people prove who they are, by doing security checks is a very good way to stop bad people from getting into financial accounts.

With all the new technology the study says that it is important for people to know about online payment fraud and how to stop it. So, to stop payment fraud we need to use new technology and have good security systems and make sure people know about the dangers of online payment fraud. If we use technology to detect and prevent fraud and if people know how to keep themselves safe online, we can make it much harder for bad people to commit online payment fraud and make the internet a safer place for everyone to use online payment systems.

Fig 3. Output of online payment fraud cause and prevention techniques

5. Conclusion

In conclusion the rapid advancement of technology and the increasing use of online payment systems have significantly changed the way financial transactions are done across the world. The use of payment systems like internet banking, credit cards debit cards and mobile wallets for financial transactions has made financial activities faster easier and more convenient for users. However, with the increasing use of payment systems the risks of online payment fraud have also increased. Cybercriminals always come up with strategies to take advantage of the loopholes of digital technology and trick users into giving them unauthorized access to their financial information. This research study aims to identify the reasons for online payment fraud and the techniques that can be employed to prevent such activities.

The findings of the study indicate that there are factors that lead to the rise in online payment frauds. One of the factors is the lack of cybersecurity awareness among users. Many users unknowingly disclose information like bank account information, passwords and one-time passwords through phishing emails or messages or through fake websites. Weak authentication mechanisms, weak passwords and unsecured internet connections also lead to cyber-attacks. The rise of e-commerce sites and payment apps has provided cyber attackers with opportunities to exploit online payment systems. The study also emphasized the role of technology in detecting and preventing fraudulent transactions. Technologies like machine learning, artificial intelligence, encryption techniques and online transaction monitoring systems have improved the ability to detect fraud transactions.

Machine learning techniques can process amounts of transactions and recognize unusual patterns that could represent fraudulent activities. Multi-factor authentication techniques can add a layer of security for online transactions. Users can prove their identity using factors like passwords and one-time passwords. Despite all these developments the study emphasized that it is impossible to eliminate payment fraud in online transactions by just relying on technology. Users need to be more aware of cybersecurity and know how to identify phishing avoid links and monitor their financial data. Better regulations are needed regarding payment systems. This research highlighted that online payment fraud is a problem that can be solved only by taking a holistic approach, including advanced technology, robust security infrastructure and awareness among users.

By implementing advanced fraud detection tools online payment fraud can be minimized, which will provide an online payment system, for users and online payment systems. To reduce the risk of payment fraud, financial institutions and payment service providers should have security measures in place to protect online payment systems. This is because online payment fraud is a problem. Using technologies like machine learning and artificial intelligence can really help. These technologies can look at a lot of transaction data to find patterns that might be fraudulent. This means that financial institutions can stop transactions away and avoid losing money. Other ways to make online payment systems safer include using multi-factor authentication, biometric authentication, encryption, and payment gateways. It is not about technology though. Online payment systems users also need to be aware of fraud and know how to protect themselves. Sometimes online payment systems users do not know they are giving away information like passwords and bank account details to people who want to commit fraud. So online payment systems users need to be taught about online fraud and how to stay online. For example, online payment systems users should not click on links that look suspicious and should only use websites for transactions. They should also change their passwords often. Not use public Wi-Fi for online transactions.

The government and other regulatory bodies have a role to play in stopping payment fraud. They can make rules for security and work with financial institutions, technology companies and law enforcement to make sure online transactions are safe. To make online transactions safer we need to watch payment systems transactions all the time report any fraud that happens and make new systems to detect fraud. As digital payment technologies get better, we also need to get better at stopping payment fraud. Research, in cybersecurity machine learning and data analytics will help us make better systems to detect payment fraud. If we want to reduce the risk of payment fraud, we need to have technology, rules and online payment systems users who know what they are doing. In the end stopping payment fraud is something that financial institutions, technology

providers, governments and online payment systems users need to work on. If we can make online payment systems users more aware of cybersecurity and come up with ways to prevent fraud, we can make online payment systems safer. Reduce the risk of online payment fraud.

Reference

[1] Bhattacharyya, S., Jha, S., Thereunder, K., & Westland J. C. Wrote a paper in 2011 about credit card fraud. They did a study on data mining for credit card fraud. Their paper was published in Decision Support Systems.

[2] Then I saw another paper by Bolton, R. J., & Hand D. J. From 2002. They reviewed statistical fraud detection. Their paper was published in Statistical Science.

[3] I also found a paper by Delamare, L., Abdou, H., & Pointon, J. From 2009. They reviewed credit card fraud and detection techniques. Their paper was published in Banks and Bank Systems.

[4] Jargons, J., Granite, M., Ziegler, K., Calibrator, S., Portier, P. He-Galeton, L., & Caelen O. Wrote a paper in 2018 about sequence classification for credit card fraud detection. Their paper was published in Expert Systems with Applications.

[5] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun X. Applied data mining techniques in financial fraud detection in 2011. They proposed a classification framework and academic review.

[6] I saw another paper by Phua, C., Lee, V., Smith, K., & Gayler, R. From 2010. They did a survey of data mining-based fraud detection research. Their paper was published in Artificial Intelligence Review.

[7] Sahin, Y., & Duman, E. Detected credit card fraud by decision trees. Support vector machines in 2011.Their paper was published in International Multiconference of Engineers and Computer Scientists.

[8] Whitlow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams N. Wrote a paper in 2009 about transaction aggregation as a strategy for credit card fraud detection. Their paper was published in Data Mining and Knowledge Discovery.

[9] The World Bank made a report in 2021 about Financial Consumer Protection and Fraud Prevention in Digital Payments.

[10] The International Monetary Fund talked about Cybersecurity and Financial Stability in Digital Payments in a report from 2020.

[11] The European Central Bank shared some statistics and techniques in 2019 the report is called Card Fraud Statistics and Prevention Techniques