International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Machine Learning Techniques for Credit Card Fraud Detection in Cyber Banking Systems: A Comprehensive Review

Prachi Singh
Research Scholar
Computer Science & Engineering, Sam Global University Bhopal, Madhya Pradesh
prachisingh335@gmail.com

Abstract-The rapid digitalization of the Indian banking sector has significantly transformed financial service delivery, enhancing convenience, efficiency, and financial inclusion. Online banking, electronic payments, and the widespread use of credit and debit cards have become integral to everyday financial transactions, ranging from fund transfers and bill payments to e-commerce and ticketing services. While these advancements have reduced operational costs for banks and improved accessibility for consumers, they have simultaneously increased exposure to financial fraud. The growth of internet banking and plastic money usage has led to a sharp rise in cyber frauds, including card-not-present frauds, identity theft, phishing, and unauthorized transactions. Credit and debit card transactions, in particular, are highly vulnerable due to their extensive adoption and direct linkage with banking systems. Despite improvements in fraud detection mechanisms and authentication technologies, cybercriminals continue to exploit system vulnerabilities using sophisticated techniques. This study highlights the evolution of digital banking in India, examines the nature and risks of financial transaction frauds—especially those involving credit and debit cards—and emphasizes the need for robust security frameworks, advanced authentication methods**,** and continuous technological innovation to safeguard digital financial ecosystems.

Keywords-Digital Banking; Financial Inclusion; Online Banking; Credit Card Fraud; Debit Card Fraud; Plastic Money; Cyber Fraud; Electronic Transactions; Banking Security; Fraud Detection Systems

I INTRODUCTION

The majority of consumers now use online banking as their default method of transferring funds. Insurance premiums, transportation tickets (train and bus), utility bills (including power, water, and property taxes), online purchases, and more are all being paid for by an increasing number of people through online banking. The effectiveness of internet banking has been steadily rising. One major drawback of this growth is the increase in fraudulent activity. Banking conducted entirely online, sometimes abbreviated as "e-banking" or "Internet banking"," expanded swiftly in the years preceding the current era [2].These days, a concept called "digitization" has a huge impact on the younger population. Having this digital literacy understanding has far-reaching effects on many economic areas, including banking, finance, insurance, and more. In order to provide their customers

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

with first-rate services and future income opportunities, the Indian banking sector should put digitization at the top of its priority list. This is due to the fact that digitalization is vital to financial inclusion [1].

These days, even the typical person can't live without online banking. The ability to manage one's financial accounts online is known as electronic banking, and it is a relatively new service provided by banks. Online banking facilitates a wide range of financial transactions, including those involving ATMs, direct deposits, EFTs, automatic bill payment (ABPs), and countless more [3]. This strategy also has more upside for the financial association. But compared to the conventional banking approach, this one is cheap, and it offers personalized convenience and adaptability. The risk and attacks of fraud data settlement presented numerous hurdles to this improved growth of the internet banking infrastructure [4]. Online banking security is vulnerable to hackers nowadays due to the proliferation of hacking techniques. The number of fraudulent attacks and activities has skyrocketed alongside the proliferation of online application providers serving the business-to-business and business-to-consumer markets. In this light, robust authentication methods for use in online transactions are absolutely necessary. Security of cryptographic systems has become increasingly important as information and communication technologies have progressed and become more widely used.

Financial Transaction Frauds via Credit Card and Debit Card

The Internet has had a significant impact on the business environment. Before, you had to go to a local business or place a mail order in order to make a purchase. However, this has changed significantly over time as more individuals choose to buy and sell online. In actuality, a lot of individuals opt to purchase goods and services online in order to avoid the commotion of crowds. Additionally, the way people pay has changed significantly over time, with more and more people utilizing credit cards to make purchases online. [5] On the other hand, advancements in technology have led to the replacement of physical cash with hard plastic money methods, mostly referring to credit and debit cards for the ease of daily transactions. Without a doubt, it has replaced cash transactions worldwide and has become a popular way to make quick money. Banks and many other business operations have been raised by plastic or polymer money, which has grown so ubiquitous in global society that it is now hard to imagine an economy functioning without it. The great advantage of plastic money is that it makes it possible to get credit almost anyplace without having to go to a bank or exchange money. Everywhere they go, travelers no longer have to worry about carrying and safeguarding significant amounts of cash. Using a debit or credit card allows them to pay conveniently and get the best exchange rate. Plastic money is always and everywhere accepted.

The local Automated Teller Machine (ABM) can provide instant cash, even in the middle of the night. Nowadays, everything can be bought online from the comfort of one's own home. It saves a great deal of time searching and travelling. Buying movie tickets or performances in advance with plastic money allows one to avoid huge waits. One click may be used to book and reserve hotels,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

trains, and flights. Both the buyer and the seller benefit from it. In actuality, consumers who pay online save money. The use of plastic cards or payment cards has increased as banks offer round-the-clock customer service. Since banks and other financial institutions have said that they regularly improve their financial fraud detection systems for their customers, credit card security is also not seen as a significant problem these days. These days, many just use their cards to transfer loans and EMIs. The researcher's analysis indicates that the average transaction value of credit and debit cards has increased, with credit card transactions totaling 4026.57 billion and debit card transactions totaling 3663.78 billion. Additionally, the analysis shows that by 2024, there would likely be 1740.50 million credit cards in use, compared to about 156.6 million debit card users. Numerous credit card firms, such as Visa, American Express, MasterCard, and Discover, have distributed approximately 2.8 billion credit cards worldwide. [] That being said, this is not entirely accurate. The growing use of plastic money has created problems for both the business community and consumers, regardless of how much credit cards are believed to be safer and more secure against fraud than debit cards. It's a common misconception that credit cards are less susceptible to financial fraud than debit cards since the latter are not directly connected to bank accounts. However, in the perspective of cyber fraudsters, these rapidly increasing numbers are nothing short of a holy grail. In the modern world, credit cards are great options for payments, much as debit cards. The primary distinction between the two cards is that the credit card is connected to a bank's line of credit, which functions similarly to a loan. A debit card, on the other hand, quickly and conveniently takes money out of a known bank account. [5] Credit and debit are the most vulnerable activities in terms of security; hence the biggest risks are also focused on these two processes.

The use of a falsified payment tool, the manipulation of payment instrument communications, and improper crediting are among the threats. The other two actions are less critical, and the chance of a security breach occurring during these procedures is far lower. Clients and merchants both own physical equipment such as smart cards or personal PCs. Merchants connect with their clients as well as their acquiring bank or another point of collection, such as a third-party payment processor. Issuers receive funds in return for prepaid balances provided to clients and govern the system's "flow," which provides financial backing for the "worth" delivered to consumers. In other cases, other intermediaries, like as banks, shops, or service providers, 2 may transmit stored-value equipment and holdings directly to users. A centralized house or system operators may be part of the system. With the onset of Liberalization, Privatization, and Globalization, the Indian economy has grown. The banking industry is no exception. Following 1990s financial sector reforms, information technology and computer applications changed India's banking business. ATMs (Automated Teller Machines), Online Banking, Credit Cards, PC Banking, Debit Cards, Smart Cards, and other e-banking products and services have largely replaced traditional banking. [6]

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Financial Frauds

Both the investing industry and daily life are significantly impacted by bank crime. Fraud is defined as any deceptive conduct carried out by a person with the goal of obtaining something unlawfully. The perpetrator of fraud deceives the victim in order to obtain a benefit or value. The majority of fraud occurs in the real estate sector, particularly during the purchasing and selling process as well as when tampering with insurance and tax records. Even though individuals, organizations, and even businesses frequently engage in such activity, it is uncommon. Fraud may have an impact on living expenses, savings, and industry trust. Financial institutions use a variety of anti-fraud strategies. Because they are flexible, fraudsters come up with new ways to get over security measures. Despite efforts by the government, banks, and law enforcement, economic crime still happens. The scammers of today could be a highly inventive, intelligent, and quick bunch. This thesis contrasts machine learning and other fraud detection techniques. Large data sets are also used to reveal hidden realities. Furthermore, new and innovative methods of detecting fraud are constantly being created and used to other industries due to the enormous increase in fraud that affects the financial industry every year.[7]

E-Commercial Frauds

E-commerce fraud, unlike other types of fraud in the market, takes place only on e commercial platform that is also a space to stolen or forged credit cards, the use of false identity and affiliated fraud advertisements. An online fraud commitment makes use of personal and credit card fraud information if the card is absent during this mischief process. Basically, here it means that hackers rely on the cards and its owner's information rather than depending on the physical card. These valuable details once stolen are sold in the black market to extract all money from the victim's bank account. Besides any criminal or 3 consumer frauds, the friendly fraud is one of its kind, where the victim receives a chargeback from his/her so-called friend so as to receive free goods and avoid payments. E-commercial prevalence is uncommon these days while owing substantial evidences, etc. As a result, ecommerce fraud prosecutions are uncommon, thus it's important to invest in a high-quality fraud detection and prevention management system for obliterating fraud on a platform and minimizing its financial effect. Ecommerce fraud is smart and developing, with fraudsters employing increasingly sophisticated strategies in every preceding year. [8]

Victimization of Credit and Debit Card Frauds

Although e-commercial scams employ a wide range of tactics, their most recent goals have been to create ingenious ways to get handicapped customers' credit cards. Theft of money from consumers using their credit or debit cards is known as payment card fraud. As we shall see later, there is now a strong incentive to create technological methods for specifically identifying credit card fraud. Before delving into the technicalities, there are two main types of payment card fraud: card-present fraud, which has become less widespread, and card-not-present fraud, which is more common. A number of accommodating practices appear to occur without the cardholder's acknowledgement. Millions of

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

bank accounts have frequently been caught as a result of database security breaches that have exaggerated excessive internet bills. It should be noted that even if the cardholders who were hacked attempt to report their card as soon as possible, the data that was taken from the compromised account is subject to the fraudster's permanent storage and cannot be readily tracked. Upon request, the financial institution restricts all payment channels that the fraudster may use shortly after a cardholder's account has been compromised. Because the fraudsters have a lot of information on the card and the cardholder, if the victim chooses to create a new bank account almost away after the attack, there's a potential that the account is still vulnerable and might be defrauded again. In these situations, it's also advisable to wait for the designated investigative team to provide the all-clear before opening another bank account shortly after the account breach. Cardholders must continue to reduce the risk of fraud by routinely checking their accounts, as they might not even be aware of fraudulent activity until they receive a statement. This does not guarantee that the unexpected or inexplicable actions will be detected. Victims who report quickly are able to get admitted to their respective banks in earlier situations. Fraud may have an impact on living expenses, savings, and industry trust. Financial institutions use a variety of anti-fraud strategies. Because they are flexible, fraudsters come up with new ways to get over security measures. Despite efforts by the government, banks, and law enforcement, economic crime still happens. Unlike debit cards, credit cards are not linked to bank accounts. The funds in the account are exhausted when a debit card is used illegally. However, since a credit card stores credit limits rather than real funds, it does not have this issue. Every credit card user has their credit card restrictions imposed by the issuer based on their income and creditworthiness. The user uses these credits to pay for expenses or to buy goods and services. This is the same as using the issuer's funds for a transaction. Therefore, after the issue has been found, the lender will restore credit limits even if they have been damaged by unlawful use of a credit card.

Since it lessens the possibility that credit card users' cards will ever be discovered, this seems like a fairly defensive tactic. [9] The idea of executing financial transactions electronically without the need of actual currency is referred to as credit. Credit and customer information are stored on the thin credit card. These cards stand out for their rapidly expanding e-banking capabilities, which are utilized for online money transfers and e-business transactions. The use of these cards has rapidly increased, leading to several fraudulent incidents. Credit cards are used by fraudsters to make unauthorized transactions, which causes large losses for both customers and businesses. On the other side, the development of counterfeit cards has facilitated criminals' ability to conduct transactions. Suspicious transactions are categorized as either conventional or counterfeit by credit card fraud detection. A transaction that is carried out without the cardholder's knowledge is known as credit card fraud. Online fraud and offline fraud are two types of credit card theft that occur simultaneously. The fraudsters may conduct their business online, over the phone, or with a credit card that has been stolen. [10] There are probably a lot of different kinds of credit card frauds in the

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

industry nowadays.

II CREDIT CARD FRAUD TYPES

Application Fraud

Application fraud generally refers to the bank account opened using the stolen documents such as utility bills, bank records, etc., without the acknowledgement of the true owner. The use of falsified documents during signing up an account allows fraudsters to easily withdraw money in the victim's name. The only way one can protect his/her personal information is by preserving the critical papers in a secure area, and disposing personal identifying information with caution.

Social Engineering Fraud

A fraudster executes social engineering fraud by simulating someone else and securing a consensual financial transaction or data to the scammer. Fraudsters use more complex tactics to defraud corporations and organisations. Sending fake emails imitating a senior employee is a frequent way to mislead peers into funding a fraudulent savings account. Fraudsters might impersonate a bank or payment processor to gain personal information. Phone phishing is a common social engineering tactic. Businesses may protect themselves by requiring several pre-processing phases for cash transfers and a call-back to clearly indicated contact information rather than the payment request contact information. Any illegal payments must be reimbursed to the bank's customers. It may withhold a refund, however, if it can demonstrate that the customer authorized the transaction, acted willfully to be at fault, or failed to safeguard his or her personal information that facilitated the transaction.

Skimming

The theft of sensitive data from a trade that seems to be valid is known as skimming. Photocopying receipts or utilizing a tiny electronic device (skimmer) is generally used to retrieve the victims' card number. In restaurants, cabs and other luxurious places the skimmer hides the victim's card. The card security code, which really is three or four digits long and not printed on the magnetic strip, can even be secretly entered by the burglar using a small keyboard. Call centers are another typical location for skimming. Skimming can 6 occur when third-party receipt technology is placed outside or near to a receipt endpoint. This device allows a criminal to gather a client's payment details, particularly their PIN, among each code scanner. A typical consumer needs to strive on detected skimming, but the issuing bank can easily see it with the right random samples. The insurer generates a list of individuals having identified as unauthorized claims and uses business intelligence for identifying links that are in-between the individuals and the visited establishments. Refined automations also detect fraud patterns but also ensure endpoint securities, where the breached penalties tend to consider hefty ranges by the issuances completely withdrawn from expensive ecosystems. It is disastrous businesses if it relies significantly on restaurants and other credit card purchases. Skimming entails placing a gadget over an ATM's card slot and scanning the magnetic strip when a

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

card is inserted accidentally. With a tiny camera, these devices steal a user's PIN. Europe, South America, and Argentina use this tactic. [11]

Phishing

Phishing occurs whenever a genuine user's sensitive data, such as user id, card number, password, and other credit card information, is gained throughout a false SMS or email and used in illegal or unknowing online purchases. In such situations, the victims frequently receive spam messages or emails requesting personal details, as well as false links so that the fraudsters can secretly install the malware virus for gathering that victim's sensitive data. In order to acquire such details, these fraudsters try masquerading themselves as if they were one of the sources of a legitimate company. [11]

Unexpected Repeat Billing

When online payments are progressed using personal bank account, recurring bank charges are charged in repeated billings. These are banker or customer instructions to pay a monthly payment to the payee. E-commerce vendors and payees in the US may accept Automated Clearing House (ACH) direct debit payments. Some payments or purchases are Rogue Automatic Payments.

Credit card fraud, in another way, targets utility customers who are approached unwontedly via telephone calls, or emails by people posing as customer care representatives. These posers try to manipulate the users into believing that their services are interrupted and can be resolved by completing an immediate reloadable debit card payment. These exploiters even try to lure victims into believing them by utilizing realistic-looking phone numbers and images.

Clean Fraud

The term "clean fraud" is neither clean nor suitable, that uses - credit cards for conducting transactions while assuring that the offenders can bypass financial firms' theft detection systems. The offender then uses the stolen card for completing illegal purchases using that same card owner's personally identifiable data. [12]

Triangulation Fraud

The criminal creates a bogus online retailer for offering low-cost goods and services. These websites collect credit card info from web users. The unscrupulous party acquires the item from the legitimate website or merchant and has it sent to the consumer using the stolen credit card information. Because the impostor obtains money for the items, the buyer is forced to pay twice. One for the fake store's pricing, and one for the genuine merchant's price. [13] With technology upgrading each proceeding day, the list of credit user continues to keep increasing along with the popularity of online shopping. While debit cards are clearly only used for direct, modest and infrequent transactions. Credit cards, on the other hand, are widely used for purchasing expensive items either on an online or an offline retail or e commercial store or to clear off debts in installments. Following suit is an unwanted increase in an anticipated credit card fraud. Forbes specifically states how online frauds are on a great rise since past few years, that even talks about the boost in the number of card-

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

not-present (CNP) credit card transactions by consumers as well as businesses that often leads to creating a bigger quadrangle for the scammers and experimenting loots with new approaches. Over the years use of credit cards has increased and technology has changed, so has the fraud pattern. Today, Card-not-present is one of the significant 8 financial frauds carried out amounting to financial losses of 1.43 billion pound in 2018. [14] The purposeful use of illegal transactional methods or credit card detecting fraud strategies must be mentioned, followed by an explanation as to how a credit card validation operates, because every malicious attack leaves a trail.

Credit Card Authorization Process

Whenever a business acquires a validation from a bank that issued credit card for payment that process is referred to as an "authorization". In other words, when a customer's card issuing bank requires consent from its owner in order to carry the further transaction process. That process is considered as an authorization that reserves sale amounts only if accepted by the bank. If the store does not satisfy Visa or MasterCard criteria controlling approval protocols, reimbursement to the merchant do get delayed or may be charged back at a later date. The authorization is granted in real time as the transaction occurs.

The Figure. 1.1 below depicts the various clearance replies that may be received from an issuer, as well as the actions and responses that need to be taken into consideration. [15] Merchant swaps the card and sends information to Merchant bank Cardholder presents card. Credit Card Network sends request to card issuer Credit Card Network sends back response to Merchant bank Merchant Bank send authorization request to Credit Card network Credit Card Issuer Approves or Declines the transaction. Merchant completes the transaction on the basis of response received Merchant Bank sends back response to Merchant The exact verification processing operations differ from one payment gateway to the other one along with the one from that of the merchant, but the scope is the same:

A cardholder purchases something from a merchant. The authorization and transaction process begins whenever an order is placed by the cardholder at an offline retail store, on an e-commercial website, etc. For completing the payment process, these sources require its customer to enter certain bank account details such as name and address registered at the respective bank, card account number, card expiration date, card verification code, and payment amount. Payment data transmission to the issuing bank. The acquiring bank obtains the cardholder’s payment information (also known as acquirer, merchant bank or processing bank). The acquiring bank requests Visa or MasterCard authorization. The payment details are forwarded by the issuing bank to the relevant Credit Card Association that subsequently authorizes the operation. Credit Card Association sends card issuer a validation request.

Card issuer authorizes or rejects transaction. Once the card issuer has made its authorization decision, the answer is returned to the merchant via the usual channels. A positive validation response indicates that the account has money in it and neither has been detected as lost or stolen.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

However, there has been hardly any proof regarding the fraudulency with that particular credit card; consequently, matching with its signatures and guaranteeing sales receipts to confirm whether a particular customer is a valid user or not. 10 Transaction Cycle of Master Card: Transaction Initiated: The moment the Cardholder makes a purchase from the merchant, the transaction begins in earnest. Authentication: The merchant essentially "sells" the transaction to the "acquirer" and receives a reimbursement for the amount of the sales ticket less a "discount charge." Transaction Submitted: For completing the payment process, the transaction needs to subsequently get submitted to the respective issuing bank via the settlement and interchanging systems of the MasterCard. Merchant Payment: The bank pays the merchant acquirer through the MasterCard settlement system, excluding the interchanging charge that substantially compensates the issuance for its expenditures. Cardholder Payment: Lastly, the cardholder ends up paying the issuer for the items or services they originally had purchased from the merchant.

Types of Financial Fraud Detection Techniques

Financial fraud is a huge issue that affects both daily life and the financial sector with a bigger impact on integrities, confidences and lifestyle of the finance sectors and customers respectively. Financial frauds can only be avoided by identifying abnormal activities from initial transactional behaviours. There have been numerous ways to recognise frauds that are usually ineffective because of new-edge technologies and schemes used by the scammers for completing a forgery. Facts prove that every internet based commercial system is that includes online transactions, such as banking services, is susceptible and sensitive to fraudsters. As a result, anti-fraud has aroused the interest of many scientists who wish to understand more about the issues that this industry faces. The gravity of the fraud problem spurred scientists for developing technologies for detection and even assessing fraud risk. Data mining extracts relevant information from a dataset using statistics, machine learning, mathematics, or AI. Financial fraud approaches include Nave Bayes, Support Vector Machine, Linear Regression, Logistic Regression, K-Nearest Neighbors, Decision Trees, and Random Forest. Classification, visualization, outlier detection, clustering, regression, and prediction, to mention a few, are six of the areas that predictive analytics might fall under and are frequently used for detecting financial crimes. Furthermore, it is claimed that one out of every three firms has been the subject of a large-scale fraud operation in the previous two years. Surprisingly, it is just the 10% of the financial frauds that hardly are uncovered by happenstance. Several studies have estimated that in year 2018 the annual cost of financial was of $27.85 billion which is likely to reach to $35.67 billion by 2025. [11] Aside from that, financial fraud has far-reaching societal effects, since it may be used to support unlawful activities such as organized crime and terrorism. Because the majority of firms want to participate in the fight against fraud, they must put in place suitable systems and processes for detecting frauds early on, or even before they happen.

Proactive and reactive fraud detection strategies, as well as manual and automated fraud detection techniques, are broadly split into two categories. In organizations that rely on IT systems to support

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

business activities, corporate data is now widely controlled and kept by IT systems. As a result of such technologies, the amount of human connection has been lowered to a larger extent, which has become the primary source of fraud in an organization. Organizations use automated controls to identify and prevent such scams. In the current situation, technology is both a blessing and a burden for humanity. While experts throughout the world devote their lives to developing a new formula or technology to identify such fraud, geniuses in every part of the globe are busy devising new ways to steal or exploit another bank card. A clever fraudster may get through even the most efficient detection method.

As a result, the company must be highly astute in establishing fraud detection tools. [16] A severely impermeable barrier that can stand against the credit card frauds is both the card-present and card-not-present conditions. They can be constructed using machine learning, and is equally known at this current stage to be one amongst the most other productive frequent methodologies for identifying abnormalities in data fraud pattern behaviours. [17]

Many internal auditors have serious faults; the primary motive for utilizing data and insights is to prevent fraud. Numerous law enforcement agencies, for instance, already employ corroborating evidences or charges from informants for identifying corporations engaged in suspected fraud cases. The vast majority of deceptions therefore go undetected, unreported as well as un-penalized. Businesses and organisations utilize data mining, data matching, and sounds like function, Regression analysis, Clustering analysis, and Gap to test, detect, verify, fix mistakes, and monitor control systems for fraudulent activity. [18]

Banking

The banking segment is the lifeline of various current economies. It is the significant financial pillars of the financial segment, which plays an essential role in economic functioning. Moreover, it is the most significant one for the economic progression of a country, and its financing needs of trade, agriculture, and industry are assembling with a high degree of responsibility and commitment. Therefore, the progression of the country is integrally associated with the expansion of banking [5]. In the current economy, banks are considered not as a trader in money but as leaders of progression. The banking system also plays an imperative task in the mobilization of payment and deposits of credit in several segments of the economy. Normally, the banking structure replicates the economic health of a country

The power of an economy relies on the effectiveness and strength of the financial structure, and it depends on a solvent and sound banking scheme. The sound banking method is effectively organized in dynamic segments and also solvent banking structure guarantees that the bank is proficient to meet its necessities to depositors [6]. The progressing technology in the banking segment has major inferences for banks marketing efforts, particularly in digital banking customer interface .Along with this, digital banking through mobile, internet, and telephone becomes the main method for delivering multi-channel services to customers, and it a challenging one as compared with the traditional

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

banking system. The digital banking system enlarges the customer expectations in which productivity improvement is a significant one [7].

Digital Banking

One innovative industry is digital banking, sometimes known as electronic banking. Customers may manage their money from anywhere in the world thanks to the internet. The electronic banking system deals with various expansions, to name a few, client demand for anywhere, anytime services, product time to market essentials, and difficulty of bank office integration problems

The digital banking system permits the customers for accessing their banking account, demand a current account statement, reorder checks, product information, observation of current bank rates, and accessing latest transactions. Along with this, various banks, namely Citibank, Fleet Financial Group, Royal Bank of Canada, Chevy Chase, Bank of America, Mellon Bank, KeyCorp, Michigan National Bank, Bank One, Bank, Comerica, First Bank Systems, and so on are presently providing these services. The electronic banking system is normally considered as an expansion of present banking system. Moreover, Internet banking is termed as any user with browser and computer can be linked to their bank website for performing various essential banking operations. Besides, the bank has a federal dataset, which is web-enabled in digital banking. Internet banking is a borderless entity, which allows performing all banking services at anyhow, anytime and everywhere [8].

In modern days, internet banking is the most advanced technology in the economic section. Internet banking systems enables bank customers for obtaining contact with their accounts and general information on bank services and products. The internet banking system utilizes bank websites without involvement or difficulty of original signatures, faxes, telephone confirmations, and sending letters [9]. Furthermore, internet banking is the type of service in which customers can perform most retail banking services, like inter-account transfers, balance verification, and reporting any issues by means of telecommunication network without leaving their home or present location of the customers. Additionally, it offers a global connection from various positions and it is commonly accessible from every internet-connected computer. Even though, internet banking has various advantages there is a problem, termed as security. Security is a significant one in the electronic banking service. Even though, electronic banking is a modern technology, which has various capacities and also several potential issues, so some users may hesitate to use this type of systems [10]. The number of malicious applications targeting online banking transactions is enlarged significantly in current years. Moreover, there are several digital banking services, like real-time gross settlement, interbank mobile payment system, credit cards, mobile banking, debit cards, national electronic fund transfer, and so on are offered through the banks to its customers [11].

III SECURITY IN DIGITAL BANKING

Any digital banking service faces the formidable problem of security. An extremely intricate and perilous process exists for a thief to follow in the early stages of attempting to steal someone's money. Having said that, if a customer provides enough personal information, identity fraudsters can

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

simply access their online bank account and steal funds. Of the many forms of privacy, the most fundamental are physical, geographical, informational, and communicative. [12]. primarily talk about people's ability to govern their own information, we're mostly referring to their ability to maintain privacy on the Internet. People also lose a great deal of control over their personal data and how it is used, which is an offensive violation of privacy. Besides, information security includes major three sections, such as availability, integrity, and confidentiality. The Certified Internal Auditor (CIA) is generally utilized benchmark for assessment of information system security in an e-commerce environment. These three elements of security may affect through purposeful human causes, technical problems, natural occurrence, accidental, and so on. Confidentiality is termed as the limitations of information access and confession for official users and avoiding access by unauthorized users. Additionally, confidentiality is a declaration in which information is only shared between authorized organizations and persons. Authentication techniques, such as passwords and user identifications are utilized for identifying users and it helps to achieve the intention of confidentiality. Furthermore, other control techniques, like limiting every identified user access to data system resources are utilized for maintaining confidentiality. Along with this, security against spam, malware, other attacks, spyware etc., are most significant to confidentiality [12]

Normally, security is the most important problem in industrial bank management and it is linked to the huge amount of bank activities. Moreover, the security of banking is ensured by computing different aspects. Apart from this, business-related bank security is a difficult structure, which includes several performances, like resource organization in the context of operational risks, market, and credit. Process security is mainly persistent on working risk and it is called the risk of failure resultant from external conditions or internal processes.

Physical security is associated with the security of money in ATMs and bank branches. The security of the system involves every exterior and interior process, which is realized through an information system [13]. The security of customer deposits is the key feature of banks and highly manipulates preservation, loss, or acquisition of customers. Therefore, it is significant for the commercial bank as the business element for undertaking various measures for ensuring suitable and effective protection of customer’s deposit [14]. Electronic banking is referred to as the body of the-information measures, which permits remote access to bank account .Electronic banking is a structure of offering banking services through electronic devices, like mobile phones, landlines, and computers. The electronic devices are utilized to accept cards, which is performed with no concurrent presence of both parties via data transfer at the request of the customer. The customers receive and transfer through devices that are particularly designed for electronic processing. Moreover, through this electronic processing method, the data are transmitted via telecommunication networks. The bank customers can perform active and passive operations and their types are dependent on the type of contract performed among customer and bank [15].

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Fraud Detection

One strategy for detecting fraud in online banking makes use of the widely used Wisdom Web of Things (W2T) approach [16]. Included in the multi-feature data it offers are details about digital banking customers' demographics, electronic fund transactions, credit card transactions, and other pertinent data kinds. This multi-faceted data is sent to the data center via the Internet or the WWW. This data center provides the infrastructure necessary to detect and prevent online banking fraud. By merging their respective functions, clients and computer systems are better able to understand and work in tandem with one another in online banking. Fraud prediction is a crucial task in this W2T data cycle. Since many customers don't check their online banking history often, it can't identify and report fraudulent transactions right after they happen. There is extremely little chance of loss resurrection as a result of this technique. Even more tedious is the fact that each detection system alarm necessitates human examination. Proper identification for online banking necessitates a high detection rate, precision, and minimal false positives. There are two primary ways in which fraud can manifest: offline and online.

- **Offline fraud:** Wallets and purses are the most common vectors for offline fraud, because they often include numerous crucial documents. These papers contain vital information such as names, bank account data, dates of birth, and transaction slips; they are examples of identification cards, credit cards, debit cards, driver's licenses, and so on.
- **Online fraud**: Through this technique, fraudsters pose as legitimate websites in order to steal sensitive customer information and make valid purchases from their accounts.

Two main strategies are typically employed to combat fraud: avoiding it and recognizing it when it occurs. Preventing fraud is the first step in securing transactions that pose a high risk. Credit card fraud protection also makes use of a number of authentication techniques, such as the expiration date, the cardholder's address, signatures, and identifying numbers. Beyond that, there are two types of detection methods, such as anomaly discovery and abuse recognition [17]. In order to identify fraud, anomaly identification typically relies on regular transactions. Misuse detection also relied on tagged transactions to spot fraudulent ones. Businesses are increasingly moving toward electronic monetary transactions as part of the cashless economy, which is being used to accurately reorganize fraud.

The initial step in identifying fraudulent activity is often to observe the cardholder's purchasing behavior. Using a misuse detection type is one approach to identify potentially fraudulent incoming transactions. As a result of their extensive training, misuse types are typically familiar with the many forms of deception employed to develop modern techniques. Likewise, comparing the cardholder's past transaction data with the anomaly detection type, profiles of their typical transaction behavior can be built. If there has been any fraudulent activity, anomaly-based fraud detection can determine it by comparing the new transaction to regular transaction patterns.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Credit card fraud is another prevalent type of unlawful financial transaction. Credit cards, a type of synthetic card, are one of the payment options provided by banks to its clients using a credit card allows users access to a plethora of online marketplaces and buying options. When someone else uses another person's credit card without their knowledge or consent, it is considered this kind of credit card theft. Due to the extensive usage of credit card systems and the absence of adequate security measures, businesses lost one billion dollars to credit card fraud.

Accurately estimating losses is challenging since credit card firms are reticent to divulge information. Credit card use without stringent security measures results in billion-dollar economic losses.The worldwide monetary losses due to credit card theft reached $22.8 billion in 2017 and are projected to rise steadily until 2022. Two main types of credit card fraud exist: application fraud and behaviour fraud [18]. Application fraud occurs when an applicant applies for a new credit card using false information and the issuer approves the application. Furthermore, fraudulent activity, including credit card transactions, occurs after the card details have been correctly entered. Financial institutions and cardholders alike face the pressing issue of credit card fraud detection. Research into credit card fraud and other forms of fraud detection is crucial since even a little amount of money can go a long way.

Data Mining Fraud Detection Techniques

Data mining is a solution to the problem of specialists struggling to extract meaningful information from the ever-increasing amounts of data made available by technology's ubiquitous use. The capacity to sift through large amounts of data using statistical algorithms in order to find correlations and patterns is known as data mining [23]. For the most part, data mining can lead to better understanding and utilization of the data by discovering and extracting friend data nuggets from corporate data warehouses or information that website visitors have dumped. According to [24] data mining is a subset of knowledge discovery, a more comprehensive process that lays out the processing processes needed to produce expressive results. Fraud analysis and user behavior analysis are the two main types of credit card fraud detection approaches.

At the transaction level, the methods for fraud analysis handle the supervised classification task. These techniques use past statistics to determine if a transaction is fraudulent or normal. Classification models that can anticipate whether new records are normal or fraudulent are generated from the dataset. Classification tasks such as rule induction, decision trees, and neural networks are employed to determine whether transactions are legitimate or fraudulent. This method has been shown to be effective in detecting the majority of previously observed fraud tricks second method focuses on account-level behavior-based unsupervised approaches. This system flags a transaction as suspicious if it deviates from the user's typical actions. Because the person is unaware to expect fraudsters will behave the same as the account owner or be conscious of the behavior model of the owner. With this aim, the system is need to mine the legitimate user behavioral model for each account and then detect fraudulent activities according to it. The behavioral profile may contain the

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

activity information of the account; such as amount, location, time of transactions and merchant types [25].

Some current fraud detection techniques that are applied to credit card fraud detection tasks are,

- Artificial Neural Network
- Genetic Algorithm
- Hidden Markov Model
- Support Vector Machine
- Bayesian Network

Fraud detection in **credit card transactions** relies on machine learning and deep learning techniques to identify anomalous patterns and fraudulent behaviour. Some of the most commonly used techniques include:

1. Artificial Neural Networks (ANNs)

- **Deep learning-based fraud detection** models that learn complex relationships in transactional data.
- Can detect both **known and unknown fraudulent patterns** by adapting to new trends.

2. Genetic Algorithm (GA)

- An **evolutionary optimization algorithm** used to improve fraud detection models.
- Helps in **feature selection and optimizing model parameters** to increase detection accuracy.

3. Hidden Markov Model (HMM)

- A **probabilistic model** that identifies fraud by analyzing sequences of credit card transactions.
- Effective in detecting fraud based on **user behavior deviations over time.**

4. Support Vector Machine (SVM)

- A **supervised learning algorithm** that classifies transactions as fraudulent or genuine based on historical data.
- Works well with **high-dimensional transaction data** and **imbalanced datasets.**

5. Bayesian Network (BN)

- A **graphical probabilistic model** that calculates the likelihood of fraud based on transactional features.
- Useful in **real-time fraud detection** by computing posterior probabilities of fraud occurrence.

Artificial Intelligence (AI)

Machine learning (ML) and artificial intelligence (AI) are subfields of computer science that are linked but separate from one another. When it comes to visual perception, speech recognition, decision-making, and natural language processing—tasks that are normally associated with human intelligence artificial intelligence (AI) is the field that concentrates on engineering such robots.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Robotic process automation is the process of creating computer programs or systems with the ability to reason, learn, and make judgments given certain inputs.

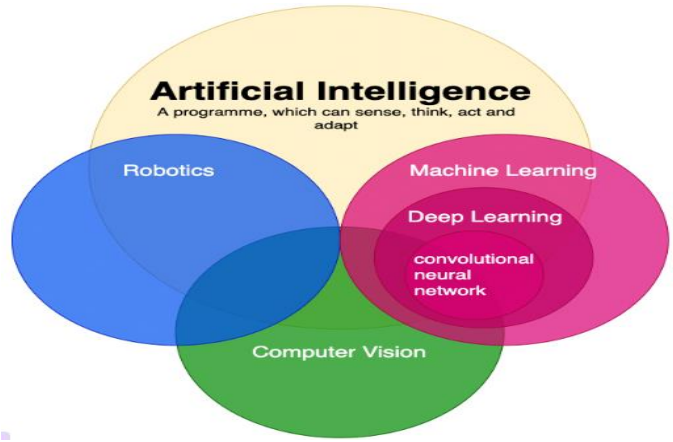

Fig. 1Artificial Intelligence (AI) Revolution

How does Machine Learning work

For the purpose of making predictions about future data, machine learning systems first develop prediction models based on the data they have learned from the past. The existence of a substantial amount of data makes it possible to develop a model that is more precise, which in turn enhances the precision of the output that is anticipated. Imagine that there is a complicated circumstance that demands predictions; rather than writing code specifically for it, we can simply input the data into generic algorithms without having to write any code at all. Using these methods, the computer will be able to construct reasoning based on the data and make predictions about the next output. Back in the day, we took a different approach to the problem, but machine learning has completely transformed that. A block diagram with an illustration of a machine learning algorithm is presented below.

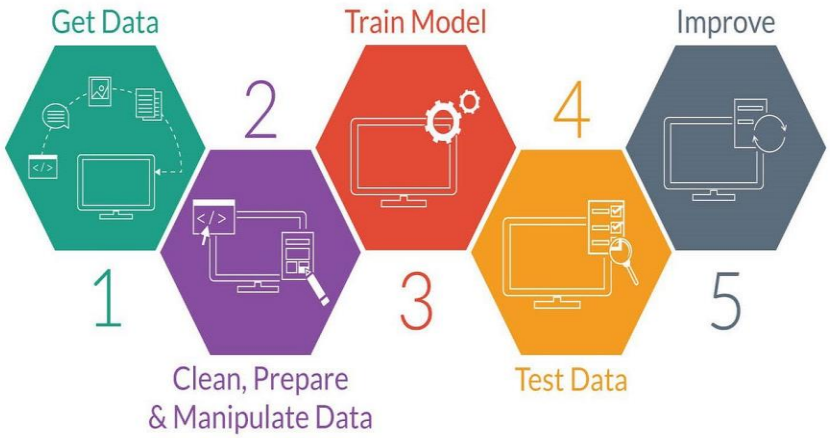

Fig 2 machine learning flow

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Classification of Machine Learning

Largely speaking, machine learning can be broken down into three groups:

3 **Supervised learning**

4 **Unsupervised learning**

5 **Reinforcement learning**

Supervised Learning

One form of machine learning is supervised learning, which involves training the system with sample labeled data and then using that data to make predictions. When the system has learned how to interpret the datasets from the labeled data, it trains and processes the model. Then it utilizes some sample data to see if it can correctly guess what the result will be. With supervised learning, the goal is to find a link between the data that goes in and the data that comes out. When a student learns anything under the watchful eye of an instructor, they are engaging in supervised learning. Some examples of supervised learning are "spam filtering" for example. Two groups of supervised learning methods can be found:

Classification

Regression

Unsupervised Learning

Computers are able to find out how to perform tasks on their own through a process known as unsupervised learning. No labels, classifications, or categories are included in the training data set that is provided to the computer. It is anticipated that the algorithm will function independently on this data set. It is the goal of unsupervised learning to reorganize the data that is being received into new features or a collection of objects that have patterns in common. There is no known outcome associated with learning that is not regulated. The computer analyses the massive amount of data in an effort to draw conclusions. Two other types of algorithms can be distinguished from it:

- **Clustering**
- **Association**

Reinforcement Learning

One kind of feedback-based learning is known as "reinforcement learning," and it works by rewarding good behavior and punishing bad behavior. These inputs trigger the agent's natural learning process, which in turn boosts its efficiency. An agent engages in exploration and interaction with its surroundings in reinforcement learning. An agent will work to maximize its reward points by doing better and better. An example of a robotic dog that uses reinforcement learning is one that learns how to move its arms autonomously.

Fraud Detection Issues and Challenges

Fraud detection is a complex domain which may lead to have a low accuracy rate, or gives many false alarms if it is not properly evaluated. Fraud detection systems have several difficulties and

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

challenges to be faced and an effective fraud detection technique should have abilities to address these difficulties in order to achieve best performance [26].

Imbalanced Dataset

One of the key issues to be looked at in a fraud detection state of the Imbalanced environment of the dataset. In order to provide precise results, the fraud detection applications require concrete data rather than synthetic data. Being bound to the confidential law, the dataset providers will not be able to provide the data as such. Further, due to the real time nature of the data, the dataset may contain illegal values, missing or NULL values and inconsistent data and using the data as such will lead to misclassifications. Hence data should be cleaned before making it use.

Trepidation of False Positives

The major difficulty encountered in the method of fraud detection is misclassification. Though true negatives establish to be financially costly for the banks, false positives deserve heavier damages. A false positive is the one that finds a genuine transaction to be fraudulent. When response to this alert is triggered, it affects the consumer directly, which incurs spoil the good will of the organization. Hence lessening of false positives seems to be the major issue for many organizations when dealing with fraud detection applications.[27]

Emerging New Patterns of Fraud

The technology explosion has not only seen an enhance in the implementation of technology by masses, but also seen an enhancement in the mistreat of technology. As the technology advances and refined techniques for detecting and preventing frauds materializes, the system fights back using superior techniques for performing fraudulent activities, maintaining the stability. The initial detection mechanisms require statistical data mining techniques, while the current state demands further enhancements in machine learning and heuristic methods. Due to the real time

Nature of the problem, it also requires quicker results, which proves to be the biggest challenge.

Real Scenario: Big Data

Even with the obtainable real time data, developing a fraud detection system and implementing it in the real state proves to be a dispute being huge data availability and large velocity of data. Due to the increase in usage of electronic fund transfer, the number of transaction incoming processing has increased to a large degree. Further, the number of record produced per time unit has also exposed a extreme increase which results in the amplification of complexity of the detection system. [28]Hence a fraud detection system that is to be developed for the present scenario should be capable of dealing out a large quantity of records in a short period providing accurate results is mandatory.

Lack of Adaptability

The algorithms used for classification are frequently faced with the problem of detecting new types of normal or fraudulent patterns. The supervised and unsupervised fraud detection systems should apply efficient methods in detecting new patterns of normal and fraud behaviors, respectively [29-30]

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Major challenges

Digital banking is widely utilized in banking sector, even though it faces various challenges as it listed below:

Password cracking: It has different types of decryption approaches, but the most familiar type of method is brute force approach. It involves cracking of a person's password and username for the particular website through checking thousands of activities, words, names, and normal terms until the grouping of them is approved to the server. This cracking method does not need strong passwords; hence users frequently utilize common activities and names, which makes it easier for a password cracker to obtain access to the system.

Packet sniffers: The connection between the web server and the user's computer is sniffed for collecting a large quantity of data with regards to users as well as passwords and credit card information. The packet sniffers is used for collecting data and transfer it through network. However, it is very complex for identifying packet sniffers because, the main functionality is capturing network traffic data, not to control data stream.

Trojans: Trojan software is considered as most dangerous regarding electronic banking security because of its capability to connect in secret and transfers secret information. This program is introduced for the particular intention of communicating with no possibility of detection. Trojans are utilized for filtering data from various users, database systems, and servers. Furthermore, Trojans is installed for monitoring database communications, immediate messages, emails, and a large amount of another service.

Sever bugs: Server bugs are regularly established and patched in a sensible manner, which does not permit an attacker for utilizing threats besides an e-banking website. On the other hand, system administrations are frequently slow for implementing the latest updates, therefore an attacker permits adequate time for producing threat.

Denial of service attacks: By generating number of anonymous requests to the server, they will make the server performance drastically fall down. The server is requested for repetitively performing tasks, and it needs to utilize the vast quantity of server-side resources. The attackers will inject virus or Trojans on the user's Personal Computer and also instruct them for executing the attack on a particular server. Moreover, such attacks are employed by an opponent for interrupting the services. If the server is down, then, they have to access another server. This permits the attacker for installing malicious applications or disabling security configurations.

References

IV CONCLUSION

The rapid digitalization of the Indian banking sector has significantly enhanced financial inclusion, operational efficiency, and customer convenience. Services such as internet banking, mobile payments, and credit and debit card transactions have become integral to everyday financial activities. However, this digital transformation has also led to a sharp rise in financial transaction

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

frauds, particularly in online banking and plastic money usage. Cybercriminals increasingly exploit vulnerabilities in digital platforms through techniques such as phishing, identity theft, card-not-present frauds, and unauthorized transactions.

Traditional rule-based and statistical fraud detection systems are often inadequate in handling large-scale, highly imbalanced, and dynamically evolving transaction data. Although banks have adopted machine learning-based solutions, challenges remain in terms of accuracy, adaptability, and real-time fraud detection. This study highlights the urgent need for advanced, intelligent, and scalable fraud detection mechanisms that can effectively identify complex fraud patterns while minimizing false positives.

Future Scope

The future scope of this research lies in the implementation of advanced deep learning models**, particularly** VGG-19 and ANN-19**,** to enhance financial fraud detection systems.

VGG-19 Model for Feature Extraction

The VGG-19 deep convolutional neural network can be adapted to analyze transaction behavior by transforming transactional data into structured representations. Its deep architecture enables effective extraction of high-level features, helping to capture subtle and complex fraud patterns that traditional models may overlook. Integrating VGG-19 can significantly improve fraud classification accuracy, especially for sophisticated and evolving attack strategies.

ANN-19 Model for Fraud Classification

An Artificial Neural Network with 19 hidden layers (ANN-19) can be employed as a powerful classifier to distinguish between legitimate and fraudulent transactions. ANN-19 can learn nonlinear relationships among transaction attributes such as transaction amount, frequency, location, device type, and user behavior. This model can adapt dynamically to changing fraud patterns and improve decision-making in real time.

Hybrid VGG-19 + ANN-19 Framework-A hybrid architecture combining VGG-19 for deep feature extraction and ANN-19 for final classification can be developed to achieve superior fraud detection performance. This integrated approach can reduce false positives, enhance detection of rare fraud cases, and improve overall system robustness.

Real-Time and Scalable Implementation-Future work can focus on deploying the proposed models in real-time banking environments using cloud-based or edge-computing infrastructures. This would enable scalable fraud detection across high-volume transaction streams.

Explainability and Regulatory Compliance-Incorporating explainable AI (XAI) techniques with VGG-19 and ANN-19 models can improve transparency, regulatory compliance, and customer trust by providing clear justifications for fraud detection decisions.

Acknowledgement-“This manuscript can be extends with conceptual work through the empirical implementation and comparative evaluation of hybrid deep learning frameworks incorporating VGG-19, VGG-16, and Artificial Neural Network (ANN) architectures for financial fraud detection

using real-world banking transaction data."

References

1. Mbama C I and Ezepue P O, "Digital banking, customer experience and bank financial performance", International Journal of Bank Marketing, April 2018.
2. AleksandarLukic, "Benefits and Security Threats in Electronic Banking International", Journal of Managerial Studies and Research, vol.3, no.6, pp.44-47, 2015.
3. Revathi P, "Digital Banking Challenges and Opportunities in India", EPRA International Journal of Economic and Business Review, vol.7, no.12, pp.20-3, 2019.
4. Nayak R, "A Conceptual Study on Digitalization of Banking-Issues and Challenges in Rural India", International Journal of Management, IT and Engineering, vol.8, no.6, pp.186-91, 2018.
5. Dagada R, "Digital banking security, risk and credibility concerns in South Africa", In proceedings of The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic, 2013.
6. Achituve I, Kraus S, Goldberger J, "Interpretable Online Banking Fraud Detection Based on Hierarchical Attention Mechanism", In proceedings of 2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP), pp.1-6, October 2019.
7. Wei W, Li J, Cao L, Ou Y, Chen J, "Effective detection of sophisticated online banking fraud on extremely imbalanced data", World Wide Web, vol.16, no.4, pp.449-75, July 2013
8. Singh P and Singh M, "Fraud detection by monitoring customer behavior and ctivities", International Journal of Computer Applications, vol.111, pp.11, January 2015.
9. Abdelhamid D, Khaoula S, Atika O, "Automatic bank fraud detection using support vector machines", In proceedings of The International Conference on Computing Technology and Information Management (ICCTIM), pp.10, January 2014.
10. Taha A and Malebary S J, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine", IEEE Access, vol.8, pp.25579-87, February 2020.
11. Gianini G, Fossi L G, Mio C, Caelen O, Brunie L, Damiani E, "Managing a pool of rules for credit card fraud detection by a Game Theory based approach", Future Generation Computer Systems, vol.102, pp.549-61, January 2020.
12. Zhu H, Liu G, Zhou M, Xie Y, Abusorrah A, Kang Q, "Optimizing Weighted Extreme Learning Machines for Imbalanced Classification and Application to Credit Card Fraud Detection", Neurocomputing, May 2020.
13. Pumsirirat A and Yan L, "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine", International Journal of advanced computer science and applications, vol.9, no.1, pp.18-25, January 2018.

14. Omariba Z B, Masese N B, Wanyembi G, "Security and privacy of electronic banking", International Journal of Computer Science Issues (IJCSI), vol.9, no.4, pp.432, July 2012.
15. Darwish S M, "A bio-inspired credit card fraud detection model based on user behavior analysis suitable for business management in electronic banking", Journalof Ambient Intelligence and Humanized Computing, vol.10, pp.1-5, February 2020.
16. Belás J, Korauš M, Kombo F, Korauš A, "Electronic banking security and customer satisfaction in commercial banks", Journal of security and sustainability issues, 2016.
17. Gąsiorowski J, "Managing security in electronic banking–legal and organisational aspects", In Forum Scientiae Oeconomia, vol.4, no.1, pp.123-136, 2016.
18. Yazdanifard R, WanYusoff W F, Behora A C, Sade A B, "Electronic banking fraud: The need to enhance security and customer trust in online banking",Advances in Information Sciences and Service Sciences, vol.3, no.10, pp.505-9, 2011.
19. Claessens J, Dem V, De Cock D, Preneel B, Vandewalle J, "On the security of today's online electronic banking systems", Computers & Security, vol.21, no.3,pp.253-65, June 2002.
20. Mohammadi S and Abedi S, "ECC- biometric signature: A new approach in electronic banking security", In proceedings of 2008 International Conference on Computing Sciences, pp.276-280, September 2012.International Symposium on Electronic Commerce and Security, pp.763-766, August 2008.
21. Thamizhchelvy K and Geetha G, "E-banking security: Mitigating onlinethreats using message authentication image (MAI) algorithm", In proceedings of 2012
22. Quah J T and Sriganesh M, "Real-time credit card fraud detection using computational intelligence", Expert systems with applications, vol.35, no.4, pp.1721-32, November 2008.
23. Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C, "Random forest for credit card fraud detection", In proceedings of 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), pp.1-6, March 2018.
24. Bhattacharyya S, Jha S, Tharakunnel K, Westland J C, "Data mining for credit card fraud: A comparative study", Decision Support Systems, vol.50, no.3, pp.602-13, February 2011.
25. Carminati M, Caron R, Maggi F, Epifani I, Zanero S, "BankSealer: A decision support system for online banking fraud analysis and investigation", Computers & security, vol.53, pp.175-86, September 2015.
26. Shen A, Tong R, Deng Y, "Application of classification models on credit card fraud detection", In proceedings of International conference on service systems and service management, pp.1-4, June 2007.

27. Yang W, Zhang Y, Ye K, Li L, Xu C Z, “FFD: A Federated Learning Based Method for Credit Card Fraud Detection”, In International Conference on Big Data, pp.18-32, June 2019.
28. Wang, C., Wang, Y., Ye, Z., Yan, L., Cai, W., and Pan, S., "Credit Card Fraud Detection Based on Whale Algorithm Optimized BP Neural Network," In proceedings of 13th International Conference on Computer Science & Education (ICCSE), 2018.
29. Panigrahi S, Kundu A, Sural S, Majumdar A K, “Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning”, Information Fusion, vol.10, no.4, pp.354-63, October 2009.
30. 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), pp.220-226, March 1997.
31. Fiore U, De Santis A, Perla F, Zanetti P, Palmieri F, “Using generative adversarial networks for improving classification effectiveness in credit card fraud detection”, Information Sciences, vol.479, pp.448-55, April 2019.
32. Zhou, X.-H., Sheng, W.-G., Xue, Y., and Chen, S.-Y, ”Generative adversarial network based telecom fraud detection at the receiving bank,” Neural Networks, vol.102, pp.78–86, 2018.
33. Carneiro N, Figueira G, Costa M, “A data mining based system for credit-card fraud detection in e-tail”, Decision Support Systems, vol.95, pp.91-101, March 2017