JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INTERCONNECTIVITY OF E-BANKING AND CYBERFRAUDS IN INDIA

[1]Santosh Kumar, [2]Dr. Sumita Sinku

[1]Research Scholar, [2]Assistant Professor
Department of Commerce,
Mahatma Gandhi Central University, Motihari, Bihar.

Abstract: - In the economic development of a country, the role of financial sector is very vital and significant. Banking is the key element of an economy. The economic growth needs a strong and healthy banking system. The application of internet in banking organizations has renovated the banks. It has benefitted both the customers as well as banks. E-banking refers to a method that allows a consumer to conduct personal or commercial banking transactions over an electronic or telecommunication network. It has undergone a number of changes as a result of technological advancements and innovation like the introduction of the electronic card, the Electronic Clearing Service, the Electronic Funds Transfer, and the enactment of online banking and mobile banking. Due to convenience and flexibility, e-banking is becoming more popular. Cyber attackers are constantly attempting to get unauthorised access to financial and corporate information in order to commit fraud. E-banking fraud is a kind of fraud in which money is unlawfully taken from a bank account and or transferred to another bank account utilising online technologies. It is generally done using techniques such as phishing, lottery fraud scams, spam, and spyware, card skimming, and hacking. Customers easily fall into the trap of internet scams or frauds conducted by fraudsters due to ignorance or simple mistakes.

The goal of this study is to identify the various e-banking services and products available in India as well as to investigate the issues that the e-banking business faces. The study also intends to describe the various forms of cybercrimes that occur in e-banking and to examine the efforts taken to combat cybercrime in the banking industry. The Study indicates that due to the rapid advancement of technology, banks must examine their rules and strengthen their systems for getting control over cyber fraud in e-banking. Banks can educate clients about financial frauds and how to prevent them by posting information on their websites. They should take adequate steps to combat these crimes, such as hiring workers with strong IT backgrounds who are properly trained, skilled, and knowledgeable. Banks and customers win the race for a better tomorrow when they work together.

Keywords: *E-banking, Information technology, Cybercrimes, Regulations and Cyber security.*

I. INTRODUCTION

Every country's banking system plays a vital role in its economy. It is necessary for any nation since it meets the credit needs of all sector of the society. Technology has evolved as a crucial tool. In contemporary business, Today's banks work in a highly globalised, liberalised environment, a competitive and privatised environment. IT has ushered in new business opportunitiesparadigm. It is becoming increasingly important in terms of improving servicesin the financial sector. The Indian banking industry has experienced remarkable growth andadvancements as a result of broad advances in the information technology. The use of e-banking comes with several benefits. It provides a platform for banking at any time and from any location. Customers have the ability to log inaccessing their accounts via websites or cards at any time and from any location is possible without being concerned about bank opening hours or without standing in bankqueues. Customers can simply visit their banks via the internet to view their account information. It helps to create a positive relationship between the bank and its customers.

E-banking encompasses performing tasks such as fund transfers, checking account statements, utility bill payments, opening a bank account, locating the nearest ATM, obtaining information on financial products and services& applying for loans by using a personal computer, smartphone, laptop, or personal digital assistant.It is a banking arrangement in which a customer can conduct numerous transactions over the internet that are end-to-end encrypted, meaning they are entirely safe and secure.Paperless/cashless transactions are encouraged by e-banking. It also comes with a set of rights, obligations, and costs.

As a consequence of the ever-increasing usage of internet technology in everyday life, cyber security is currently the most serious problem around the world. On the internet, anyone may get knowledge on any subject. Online data communication, social media interaction, online shopping, online banking, and online bill payment are becoming essential in day-to-day activities

and the internet is required for these activities. As a result of fraudulent operations, criminals are more simply conducting cybercrime rather than physical crime. Customers easily fall into the trap of internet scams or frauds conducted by fraudsters due to ignorance or simple mistakes. It is generally done using techniques such as phishing, lottery fraud scams, spam, spyware, card skimming, and hacking.

II. REVIEW OF LITERATURE

Brar et.al., (2012) tries to investigate various risks related to e-banking and whether these risks can be totally eradicated or not. They concluded that with the help of various tools total eradication of risks is not possible but can be highly reduced if internal control measure techniques are adequately put in place. With the advent of on-line services, customer have greater choice and do not need to be tied to one financial institution or another. Clearly, the sustainability of e-banking depends on its accuracy, reliability and accountability.

Manjula and Shunmughan (2016) have analysed about the cyber space and the customer's perception about cybercrime by using sample of 120 respondents and percentage analysis & chi-square has been used as tools to analyse the data. The study concludes that more awareness programs should be conducted for the customers so that the cybercrime can be reduced in future period of time.

Chaturvedi (2017) examined awareness amongst individuals for making use of internet banking. It also attempts to analyse reasons for customers not preferring electronic banking. The study reveals that certain measures must be taken by users while using the internet to perform digital banking transaction which will help them to combat the Cyber Crime and customers should not reveal their account details via e-mails and while chatting.

Dubey and Manna (2017) focused on understanding the ways of Internet banking frauds that take place in our banking systems nowadays as well as to highlight the ways of Fraud risk management on behalf of each individual bank. The study finds that due to the advancement of technology, the fraudsters also use technology to perform fraud in new and innovative ways. So, the financial institution should develop strong fraud risk management and fraud controlling mechanisms for the development of banking services and customer trust.

Ali et.al., (2017) critically analysed and discussed the effects of cyber threats when dealing with online banking services. It can be concluded from the study that there is a need to increase customer's awareness about available cybercrimes when dealing with online banking and sensitive financial data.

Bhatt and Pant (2017) described different safety features used by the banks for online transaction and examined where the problem exists in the system. They found that all the banks use the latest technology for the online security feature but still they have small loop wholes in this feature as well as the banks don't have any user awareness program to spread information and this is one of the biggest reasons of this online security.

Jaro and Rajan (2018) identified various e-banking services adopted in India and studied about the various challenges and issues faced in e-banking. They concluded that with digitalization of Indian economy and move to transform India into cashless society, e-banking is going to be strengthened.

Rao (2019) revolved around the specialized parts of different kinds of cybercrimes concerning the saving money units and their related effects as well as identified the danger ways supporting these wrong activities. There is a need to avoid digital wrongdoing by guaranteeing validation, recognizable proof and check procedures when an individual goes into any sort of saving money exchange in electronic medium. The development in digital wrongdoing and intricacy of its examination strategy requires proper measures to be embraced. It is basic to expand the collaboration between the partners to handle digital wrongdoing.

Gupta & Sharma (2021) assessed the impact of cybercrimes on the e-banking in India by using report of the RBI and also analysed that to what extent legal provisions are effective and efficient enough for controlling the cybercrimes against e-banking in India. It can be said that the cybercrimes are increasing every year & due to increase in use of Technology and internet, Unauthorized Network Scanning/Probing/Vulnerable Services has increased drastically but Phishing, Website Intrusion & Malware Propagation have shown a decreasing trend.

Vijayalakshmi, Priyadarshini and Uma Maheshwari (2021) critically examined and explained the impact of cyber threats when dealing with E-banking facilities. It can be concluded that there is a need to increase safety measures in available cybercrimes when dealing with Internet banking and sensitive financial data also there is a necessity to aware the Internet banking consumer on how to prevent the available risks.

III. RESEARCH GAP

After making extensive and detailed review of the available literature, it has been found out that some studies deal with the conceptual overview of e-banking and cybercrime, challenges in e-banking sector. However, some research paper includes forms and preventive steps for cybercrimes. So, this study is based on interlinking of e-banking and cybercrimes in India.

IV. OBJECTIVE OF THE STUDY

- To identify the various e-banking services and products available in India
- To investigate the issues that the e-banking business faces.
- To describe the various forms of cybercrimes that occurs in e-banking.
- To examine the efforts taken to combat cybercrime in the banking industry.

V. DESIGN OF THE STUDY

The nature of the study is descriptive and exploratory and there is no use of statistical tools and techniques in this study.

VI. EXPLANATION AND EXPLORATION OF THE STUDY

Concept of E-banking

E-banking is a broad term that refers to a method that allows a consumer to conduct personal or commercial banking transactions over an electronic or telecommunication network. It is a product provided by banks that facilitates online banking and allows customers to access their bank accounts with just one click.

The varieties of services covered under E-banking are:

1. Internet Banking: A banking service that allows consumers to conduct a variety of monetary and non-monetary transactions over the internet, via the bank's website or application.

2. Mobile Banking: Almost all banks have developed mobile applications that allow you to conduct transactions on the go. A smartphone, internet, mobile application, and mobile banking service enabled in your bank account are all required.

3. ATM: Automated Teller Machines, or ATMs, are one of the most prevalent and early services offered by e-banking. It is not only a machine that allows you to withdraw cash as needed, but it also allows you to check your account status, transfer funds, deposit funds, update your mobile number, and alter your Debit Card PIN.

4. Debit Card: Debit cards are widely utilised in our daily lives to complete a wide range of transactions. Debit cards are linked to the customer's bank account, so all the customer has to do is swipe the card to make a purchase at a POS, shop online, or withdraw money from an ATM. The amount is directly debited from the customer's account in this manner.

5. Credit Card: A credit cardis like a payment card that banks offer to customers upon request after reviewing their credit score and history. It allows the cardholder to borrow and pay for monies up to the pre-approved amount. The card's limit is set by the banks who issue it. For the use of a credit card, the cardholder agrees to repay the amount within a specified time frame, subject to certain fees.

6. Point of Sale (POS): A point of sale system refers to the time, date, and location (retail outlet) at which a consumer makes a payment for a purchase or services obtained using a plastic card.

7. Electronic Data Interchange (EDI): EDI is a new way of exchanging information between businesses using a standardised format rather than the traditional paper-based method.

8. Electronic Fund Transfer (EFT): An electronic fund transfer is when money is moved electronically from one bank to another. It includes Direct debit, direct deposits, wire transfers, NEFT, RTGS, IMPS etc.

(A) NEFT (National Electronic Fund Transfer)

- It is a payment mechanism that enables for one-to-one transfers of funds.
- Individuals and businesses can transfer payments electronically from any bank branch to any other bank branch in the country using NEFT.
- The NEFT service is available 24 hours a day, seven days a week using internet banking. However, it is a limited-time service at the bank branch.
- NEFT transfers are usually done in within 30 minutes. Nonetheless, the time could take up to 2-3 hours or could be accomplished in as little as 10 minutes.

(B) RTGS (Real-Time Gross Settlement)

- It is a real-time gross settlement system that allows payments to be settled on an order-by-order basis.
- RTGS transactions are tracked by the RBI, making successful transfers irreversible.
- RTGS transactions are tracked by the RBI, ensuring that the funds are credited to the receiver's account almost immediately and not after a certain period of time, as is the case with other payment modes like NEFT. This approach is mostly utilised for transfers of big amounts of money.
- The minimum amount that can be sent using RTGS is Rs. 2 Lakh.
- The maximum amount that can be transferred via RTGS is unlimited.
- RTGS, like NEFT, is available online 24 hours a day, seven days a week.

(C) IMPS (Immediate Payment System)

- It is another real-time payment technique.
- IMPS is a system for immediately transferring funds between banks in India by mobile, internet, and ATM, which is not only safe but also cost-effective from both a financial and non-financial standpoint.
- IMPS is a low-cost method of money transfer.

- It does not require account numbers, IFSC codes, or other details that are required by other fund transfer methods such as NEFT and RTGS. The beneficiary's mobile number is also required to send money using IMPS.

Advantages of E-banking

- It allows for digital payments, which promotes transparency.
- It provides access to the bank account 24 hours a day, 7 days a week.
- It also sends out notifications and alerts to keep you up to date on financial transactions and regulation changes.
- It saves banks money on transaction costs.
- It is simple and easy for customers because they don't have to go to the bank branch every time.

Issues and risks faced by the E-banking business

1. Operational hazard

The most prevalent sort of e-banking risk is operation risk oftenly known as transactional risk. It involves the following issues:

- Wrong transaction processing
- Data integrity, data privacy and confidentiality compromises
- Unauthorized retrieval to a bank's computer systems
- Contract non-enforceability.

Human factors such as customer's/employee's negligence, employee fraud, hackersare the possible cause of e-banking operational risk.

2. Threat to Security

When it comes to banking transactions, the privacy of the transaction is significant. All customers want their transactions to be kept private. Due to online availability of information, there is always the risk that someone will access it and misuse it. Hacking threats and illegal access to the bank's systems add to the security risk of e-banking.

3. Design and Architecture of the Banking System

It is critical for the bank to have suitable system architecture and controls in place in order to handle various operational and security risks associated with e-banking. Banks are constantly at risk of selecting the wrong system architecture or technology, as well as having insufficient control processes.

If a bank's system is obsolete and cannot be upgraded, it may result in a loss of investment as well as ineffective service. To avoid any security flaws in their security systems, banks must continually update their systems to stay up with quickly evolving technology. Furthermore, the bank's employees require ongoing training to stay current with new technologies.

4. Credibility of the bank

The significance of a company's image cannot be overstated. When it comes to electronic banking, if a bank fails to fulfil important activities or fails to meet its clients' expectations, it leads to loss its reputation. This eventually results in a reduction in funds or a loss of clients.

A system or product that does not function as expected, significant flaws in the system, security breaches (external or internal), misinforming customers about the processes and policies of using e-banking, certain communication issues that prevent the customer from accessing his account, and so on are some of the reasons for this risk.

5. Regulatory threats

A legal risk exists if rules, regulations, or recommended practises are violated, or when the legal rights and obligations of any of the parties to a transaction are not established. E-banking is an extremely new industry, there is a great deal of ambiguity and uncertainty about some regulations and procedures. It puts the customers at a higher legal risk.

6. Risk of Money Laundering

The e-banking channel allows you to do all of your transactions from the comfort of your own home. As a result, standard ways of detecting and preventing illegal activity are difficult for banks to employ.While there are money laundering regulations in effect, their applicability to electronic transfers is debatable. As a result, banks are vulnerable to money laundering.

7. Risks from Cross-Border Trade

Electronic banking's primary concept is to expand both banks' and consumers' geographical reach. This implies that the expansion will be able to extend beyond national borders. As a result, there are many cross-border risks:

- Legal and regulatory risks - There is the possibility of legal ambiguity in particular nations, as well as jurisdiction ambiguities between different national authorities.
- Operational risk - If the bank chooses a service provider in another nation, it will be difficult to oversee, posing an operational risk.
- Credit risk — International transactions might raise credit risk. This is due to the difficulty of evaluating a loan application from a consumer in another country.

8. Strategic hazard

This risk includes the following threats: -

- Creating a business plan
- Having adequate financial resources to support the business strategy
- In the context of outsourced activities, the trustworthiness of the vendor
- For employees, any adjustments in the work environment;
- Technology level employed in comparison to existing technology

9. Other Threats

Other hazards associated with e-banking are similar to those associated with traditional banking, such as credit risk, liquidity risk, interest rate risk, market risk, and so on. However, because of the use of electronic channels and the lack of geographical limits in e-banking, these dangers are increased.

All of the foregoing dangers can occur as a result of design faults, insufficient technology, careless workers, and illegal system access (intentional or not). For a safe transacting environment, banks must employ the appropriate technology and systems, as well as have effective access control.

Recommendation of the RBI on E-Banking

The Reserve Bank of India (RBI) has a working committee that looks into various aspects of e-banking and suggests solutions. The following are some of the suggestions:

- In order to address security concerns, all Indian banks must adhere to a set of guidelines. This standard should also be designed by the Indian Banks Association.
- To protect data secrecy and confidentiality, all banks must implement suitable security measures. They must also utilise logical access control to put it in place.
- Banks must create anti-money laundering (ALM) technologies for reporting and querying in order to reduce the risk of money laundering.
- To create a fraud-free banking culture, banks must have an internal grievance redress system, and all banks must have an explicit security plan with documentation. Physical access control must also be tightly enforced by banks.
- Banks must establish a large e-banking network in order for rural customers to have access to financial services.

Forms of cybercrimes that occur in e-banking sector

With the increased usage of the Internet, cybercrime in the banking sector is on the rise. E-banking fraud is a kind of fraud in which money is unlawfully taken from a bank account and or transferred to another bank account utilising online technologies. Cyber fraud is a crime done using a computer with the goal of stealing another person's personal and financial information that is stored online.

Some of the following forms of cyber frauds are as: -

1. Phishing: - It is a fraudulent method of obtaining personal information such as credit card or debit card information, online banking login credentials, or account numbers from an account holder. Phishing is a deceptive attempt to steal your personal information, mainly by email. Phishing emails frequently pretend to be from a well-known company and request personal information such as your credit card or debit card number, PIN, expiration date, CVV number, cell phone number, online banking user ID and password, and so on. Its attempts can appear to come from sites, services, and companies with whom you have no connection. Phishing emails always instruct you to click a link that will take you to a site that will ask for your personal information. Legitimate companies would never send you an email requesting this information.

2. Vishing: - It is the criminal act of applying social engineering techniques over the telephone system, most typically through the use of Voice over Internet Protocol (VoIP) or mobile phones to get confidential personal and financial information from the general public for the aim of financial reward. It combines the words "voice" and "phishing." In Vishing, fraudsters call innocent bank customers/consumers claiming to be from a bank/merchant and informing them that there are issues with their bank accounts/online shopping and that they need to verify their account/KYC/online order and demand the victim's payment credentials before committing the fraud. Vishing is the sort of cybercrime that is used to commit nearly all financial cybercrime nowadays.

3. Smishing: - It is a type of criminal behaviour that use social engineering techniques. It is a hybrid of SMS and phishing. SMS (Short Message Service) is a text messaging techniqueused for getting financial information by text messages on cell phones through SMS/ Chat.

4. Spoofing: - It is the process of obtaining access to other computers on a network by having one computer on the network pretend to be another computer, usually one with specific access privileges. When a malicious actor impersonates another device or user on a network, this is referred to as a spoofing attack.

IP spoofing is a technique in which an attacker delivers messages to a computer with an IP address that appears to be from a trusted source. Cyber thieves use email spoofing to transmit phishing links or harmful attachments to recipients, posing as an official-looking email. To deceive the targets, SMS spoofing and call spoofing are also utilised to make them believe the call/SMS is coming from a legitimate source.

5. Denial of Service Attack (DOS): - This occurs when a criminal floods the bandwidth of the victim's network or spams his email box, swindling him of the services he is entitled to receive or provide.

6. Software piracy: - It is the unauthorised copying and transmission of genuine programmes or the counterfeiting and distribution of products that imitate the original.

7. Cyber Defamation: - In this process, a cybercriminal sends defamatory emails to all of the victim's contacts or posts the defamatory information on a website.

8. Credit Card/Debit Card Fraud: - Cyber criminals steal the credit card/debit card details such as card number, CVV, expiry date, PIN, OTP using various techniques such as through phishing, vishing etc. and do online transactions.

9. Online Wallet Fraud: - Cyber criminals steal some of the credentials needed to operate an online wallet, such as the login ID, password, and OTP, and use them to conduct fraudulent online transactions without the knowledge or consent of the legitimate wallet owner. In today's world, this is a very common type of deception.

10. Net Extortion: - It is the practise of copying a company's private data in order to extort a large sum of money from that firm.

11. Bot Network (Botnets)- A type of cybercrime in which spammers and other criminals take control of a victim's computer remotely and without his knowledge.

12. Cyberstalking: - The attacker pursues the victim by sending emails and do multiple visits to chat rooms.

13. Malware: - It is a term for deliberately created software code that is used to deceive, steal, or hurt users in a digital environment, such as online banking fraud.

14. Farming: - It is also known as pharming or Domain Name System (DNS) attack that is commonly referred to as DNS Poisoning. If the machine is infected with a "virus" that poisons the DNS system, the victim may be led to a bogus "Pharming Page" instead of the actual web page the next time he or she visits an online banking site.

15. Data Diddling: - It is the process by which a fraudster alters raw data in an unauthorised way before entering or processing it into a computer system, and then changes it back to its original form after processing it so that the data alteration cannot be easily traced. It's a form of cybercrime.

16. Cyber Squatting (Domain Squatting): - It is the act of registering, trafficking, or utilising a domain name with the bad faith goal of profiting from the goodwill of another's trademark. The cyber possessor then offers to sell the domain at an inflated price to the individual or corporation who holds a trademark in the name.

17.Cyberbullying: - It occurs when someone humiliates, criticises, or disrespects another person on a frequent basis over the internet, mobile phones, or other electronic methodsor intimidated through cell phones, instant messaging, e-mail, chat rooms, or social networking sites like Facebook and Twitter.

Preventive measures taken to combat cybercrime in the banking industry.

- Do not provide your financial and personal sensitive information to a bank, insurance company, RBI, IRDA, Income Tax, Police, online shopping merchant, or bank's call centre by mail, phone, chat, SMS, or Google Form. As a result, anyone posing as a requester of information could be a cybercriminal.
- Any caller posing as a bank or call centre may try to persuade you to reveal your credentials, such as your debit/credit card number/PIN/Expiry date of card/CVV number, OTP, Online banking User ID and password, UPI PIN, claiming that your account/debit/credit card/UPI, etc. will be blocked or your KYC will not be completed. Please do not respond to such requests because they are from scammers.
- Always protect the keypad while entering ATM PIN at ATM/POS facility if you don't want to be a victim of card cloning.
- Always inspect the ATM you're using before using it. Skimmers (false card reader devices) can be easily identified. Consider going away and transacting in another machine if some parts around the slot for inserting the card do not appear to be working properly.
- Pick a PIN that is simple to remember but not dependent on your birthday, anniversary, address, vehicle number, or phone number.
- Changing your ATM PIN on a frequent basis is a good idea. It's never a good idea to write it down or keep it in your wallet.
- Don't reuse your PIN across all of your cards.
- Never give out your debit/credit card number, expiration date, or three-digit CVV (Card Verification Value) to anyone, even family members.
- Always look up a bank's or merchant's phone number or email address on their official websites. Do not rely on phone numbers found in a Google search. Because scammers have already publicised their contact numbers on numerous internet sites, it could be fabricated and you could be tricked by them.
- Do not send sensitive personal and financial information by email, telephone, SMS, chatting, social media, or Google Form, such as debit/credit card data, online banking user ID, password, OTP, UPI PIN, ATM PIN, and so on.
- Do not respond to spam emails or contact the phone numbers listed in scam emails.
- Use a combination of alphanumeric and special characters in lower and upper case for your online banking password. The password must be at least 8 characters long.
- If your phone is deactivated without your permission or you receive a call about it, it's possible that someone is attempting to obtain a duplicate SIM or steal your credentials, such as OTP (one-time password) for beneficiary registration/issuing online Internet Banking/mobile banking/UPI facility.
- In the event of any of these suspicious activities, please change your passwords/PIN as soon as possible.

- Avoid making online friends with strangers and chatting with them.
- Never react to phishing emails and report them to your bank's email address as well as CERT-IN (Indian Computer Emergency Response Team) at incident@cert-in.org.in.
- Never forward a message from your cellphone to a number provided by an unknown caller or a fraudster. This technique is used by fraudsters to register the UPI of victims' bank customers on their mobile phones.
- Remote accessing apps such as AnyDesk, Team Viewer Quick Support, and others should not be installed on your mobile phone. Banks and online merchants never call you to help you solve your problem using the aforementioned apps. Bank customers are being duped by cyber via the AnyDesk and Team Viewer Quick Support apps.

VI. CONCLUSION

E-banking has become an essential aspect of the modern banking process& also becoming increasingly popular because of its lower transaction prices, twenty-four-hour services, increased transaction control, bigger volume of transactions in less time, and remote transaction facilities and involves broader range of banking products and services;

However, in addition to these advantages, the use of e-banking also possesses threats for customers as well as banks. Banks are exposed to various levels of risk. Customers who use e-banking services may also face difficulties. Customers that use e-banking services may have a higher tolerance for a system that is unreliable or does not deliver correct and up-to-date information. Customers now have more options thanks to online services, and they are no longer bound to a single financial institution. Clearly, the accuracy, reliability, and accountability of e-banking are critical to its long-term viability.

One of the most serious issues with Internet banking appears to be the security and protection of data shared between the customer and the bank. If there are benefits to the Internet, there are also negatives, just as there are to every coin. These flaws are so serious that they may have a negative impact on banking activities, which in turn may have a negative impact on customers and businesses. Although total eradication of internet scams, thefts, Spyware, and malware growth is difficult, but early identification and prevention can be highly effective if done on time.

VII. RECOMMENDATION

Consistent electronic banking education initiatives are required to keep people informed about how to perform secure online transactions. The Reserve Bank of India should continue to cut the cost of electronic banking services in order to encourage users to use it more. If all of the abovementioned techniques are used together, the security techniques will go from being successful to being extremely effective. Client trust and confidence would both increase as a result of this. There is a need for an industry-wide framework for effective e-fraud governance, regulation, and policies, with a focus on combating fraud through electronic channels.

A comprehensive enterprise-wide strategy to fraud control is required to support broader organisational compliance and risk management. This strategy necessitates an IT infrastructure that allows for enterprise-wide, real-time, and cross-channel monitoring and management.

REFERENCES

[1] Ali Liaqat, Ali Faisal, Surendran P., Thomas Bindhya (2017). The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services. *International Journal of e-Education, e-Business, e-Management and e-Learning.* Vol.7(1). pp.70-78.

[2] Bhatt & Pant (2017). Study of Indian Banks Websites for Cyber Crime Safety Mechanism. *International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181*, Vol.5(3). Pp.1-4.

[3] Brar et.al., (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. *International Journal of Computing & Business Research*, ISSN (Online): 2229-6166, Vol.3(5).

[4] Chaturvedi Vinaya (2017). Cyber Crime: Technological Blight in Digital Banking in India. *IOSR Journal of Business and Management (IOSR-JBM),* e-ISSN: 2278-487X, p-ISSN: 2319-7668 pp. 55-62.

[5] Gupta & Sharma (2021). Legal mechanism of cybercrimes against e-banking in India. *International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS),* ISSN: 2581-7930, Vol. 4(1), pp. 282-286.

[6] Jasmine Jaro and Rajan (2018). A Critical Study on Concept of E Banking and Various Challenges of IT in India with Special Reference to RBI‟S Role in Safe Banking Practices. *International Journal of Pure and Applied Mathematics*, Vol.119(17), pp.1661-1676.

[7] Manjula & Shunmughan (2016). A study on customer preference towards cybercrime with banking industry. *International Journal of Multidisciplinary Research and Modern Education (IJMRME)*, ISSN (Online): 2454 - 6119 Vol. II(I), pp.597-603

[8] Neeta & Bakshi (2019). Cyber Crimes in Banking Sector. *Aayushi International Interdisciplinary Research Journal (AIIRJ)*, Vol.6(5), pp.25-31.

[9] Rao (2019). Cybercrime in banking sector. *International Journal of Research – GRANTHAALAYAH*, Vol.7(1), pp.148-161.

[10] Rupesh, Dubey and Manna (2017). E-banking frauds and fraud risk management. *Tactful Management Research Journal* ISSN: 2319-7943, pp.20-23.

[11] Vijayalakshmi, Priyadarshini & Uma Maheshwari (2021). Impacts of cybercrime on internet banking.*International Journal of Engineering Technology and Management Sciences, ISSN: 2581-4621*. Vol.5(2), pp.30-34.