DOI: https://doi.org/10.53486/dri2023.08
UDC: 004.056:336.717

FRAUD PREVENTION IN DIGITAL PAYMENT SYSTEMS AND CYBERSECURITY EDUCATION FOR CUSTOMERS OF NATIONALIZED FINANCIAL INSTITUTIONS

KHUSHWANT SINGH,[12] Research Scholar
ORCID ID: 0000-0001-6732-055X

MISTREAN LARISA,[13] PhD, Post-Doctoral Researcher
ORCID ID: 0000-0002-4867-937X

YUDHVIR SINGH,[14] PhD, Professor
ORCID ID: 0000-0001-9953-3533

DHEERDHWAJ BARAK,[15] Assistant Professor
ORCID ID: 0000-0002-4968-6731

ABHISHEK PARASHAR,[16] Assistant Professor
ORCID ID: 0000-0002-6865-0582

Abstract: *Information Technology and infrastructural development-based technology has taken important part and different dimension in building the future of Indian Financial System, especially in transition from tradition banking method to E-Banking services. One of the important reasons why this transition took place is because of time and convenience which caters the needs of customers in ease of transacting their accounts anywhere and at any time. Since, increased in the number of online transactions has pave the way to increased online frauds and hacking. In the present scenario cyber security and protection of customers information has become the biggest challenge. Hackers and Cyber attackers have become common marvel and get easy access to customer information anywhere and anytime. Customers in many stances have becomes a prey and victim unknowingly, believing the mechanism to be a genuine one. This research paper mainly focuses on customer awareness and methods of preventing electronic frauds, cyber security and throws spotlight on chances of users who fall as target to hacking and phishing attack which are*

[12] erkhushwantsingh@gmail.com, Maharshi Dayanand University, Rohtak, Haryana, India
[13] mistrean_larisa@ase.md, Academy of Economic Studies of Moldova, Republic of Moldova
[14] dr.yudhvirs@gmail.com, Institute of Engineering & Technology, Maharshi Dayanand University Rohtak, Haryana, India
[15] barakdheer410@gmail.com, Vaish College of Engineering, Rohtak, Haryana, India
[16] parasharabhishek5@gmail.com, Baba Masthnath University, India

used to steal personal and bank information. This paper also examines the awareness of customer on digital frauds and cyber security provided by the perspective Nationalised Banks. Cyber security and infrastructure security can only be accomplished by sensing the techniques and practices of attackers and building a strong defence and security on the KYC of the bank customers. It also seeks to understand various factors that are responsible for bank fraud which are unidentified to the customer.

Key words*:* E-Banking, Cyber Security, Digital Frauds

JEL: G21, G23, C8

1. Introduction

Cyber security plays a very important part and role in Information Technology. Cyber protection has become a real concern in all entity of business. They spend heavily to ensure their security to protect information and their database this has become a greater challenge not only to businesses but also to banking sector as it plays a key role in Indian Financial System. In today's technical environment, technologies have changed the appearance of dissimilar business operation (Mistrean et all, 2021$_a$, Mistrean et all, 2021$_b$, Mistrean, 2023$_a$, Mistrean, 2023$_b$). In India, it has been recorded more than 60% of total commercial transaction are done online. This has flagged to all hues of cybercrimes in enormous forms. The tough fight against cyber-crimes needs a comprehensive and a safer approach to solve arising issues (Aithal, 2015).

Government through laws has enforced monitoring, investigation and prosecutes cyber- crime effectively through sector wise mechanisms. All over the world, Government has imposed strict laws on cybercrimes in order to prevent frauds and malicious activities.

In the realm of banking and financial transaction today Information Technology and Infrastructural development has become the prerequisite to compete in phase of national development amongst developing countries. In today's world it has transformation of development has been made through ease use of Internet of Things (IoT). The user-friendly technology, flexibility in terms of payment and transactions and also banking financial transactions have made an elastic from the way of traditional banking. Customers have started to depend on internet and websites to get information, compare and make decisions on the financial products or services of banking sector without mobility with one click (Mistrean, 2023$_c$, Mistrean, 2021$_a$, Mistrean, 2021$_b$). This is made possible because of Online and Core Banking transactional development. This has also given the way of other all possible cyber-attacks on the customer if they are not aware on the security systems and legal protections given by the Banks and Financial service sectors. With the same use of Internet of Things, it has laid a web for customers by cyber attackers and hackers who breaches and breaks the security systems with the help of the customers unawareness of these attacks.

Banks and other Financial Sectors are trying to instrument and protect customers information and defence against these attacks through layers of security protection on customers and designing many awareness programmes on Cyber Security and Cyber- Crimes (Animesh et al., 2017, Stiawan et all, 2017, Krishna, 2017).

According to Reserve Bank of India banks lost Rs.109.75 crores to theft and online frauds in the financial year 2018 (Report, 2016). Most of the cases which was registered were through their digital payment gateways. On this Basis RBI has advised banks to upgrade security at bank branches and all ATMs. Although challenges in terms of Information Technology ideas and skills seems to be fewer among customer and having a regular checks and monitoring has become more complex and challenging because of users are high and increased demand on online transaction. The cyber-attacks impact on banks and users can devastate not only personal loss but also financial loss, business loss, critical data loss, regulatory penalties, legalities etc. the attacks can be on malicious link attachments, Voice Phishing through Phone calls by faking the caller ID as Banks and Financial institutions, phishing baits, and false unsecured webpages where it captures the username and passwords. Fake money request and request for KYC from the customers from unknown sources, can be a possible cyber- crimes and attacks on the customers directly. Especially in the period of pandemic COVID-19 the rate of malicious and cyber-attacks has increased. In India, during the year 2020, the cyber-attacks have rose by almost 300% comparing the last year states the Union Home Ministry in Parliament based on the data from the Computer Emergency Response Team, India (CERT-IN). This is because of the lack of cyber security and awareness on phishing, cyber and malware attacks. Where the entire world was shifting and transforming to complete online for transactions, work, education, and other essential purposes.

Government and regulatory support and supervision.

There are significant ongoing efforts by Reserve Bank of India, MEITY, CERT-IN, IBCART, NCIIP in setting cyber security frame works, guiding, warning, and monitoring of cyber- attacks. Reserve Bank of India had, provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds through its Circular DBS.CO.ITC.BC. No.6/31.02.008/2010-11 dated April 29, 2011, wherein it was indicated that the measures suggested for implementation cannot be static and banks need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns (More, 2016, Mohapatra, 2016). Reserve Bank of India issued a comprehensive Circular on June 2, 2016, underlining the urgent need to put in place a robust cyber security/resilience framework at banks and to ensure adequate cybersecurity preparedness among banks on a continuous basis. The salient features are (Ali et all, 2017, Pradeep, 2016):

- banks to have a Board approved Cyber-Security Policy which is distinct from the broader IT policy / IS Security Policy of a bank;
- banks to establish cyber risks in real time through SOC (Security Operations Centre) and make arrangement for continuous surveillance to monitor and manage cyber threats;
- a minimum baseline cyber security and resilience framework is given to be implemented by the banks;
- a Cyber Crisis Management Plan (CCMP) should be immediately evolved which should be a part of the overall Board approved strategy;
- banks should share information on cyber-security incidents with RBI;
- banks to bring Cyber-security awareness among stakeholders / Top Management / Board.

RBI had created a cyber-cell under the Department of Banking Supervision and conducted a separate IT audit of banks covering each bank for separate cyber-security and IT audit (Lakshmanan, 2019, Sravanthi, 2016, KPMG, 2017). RBI is also has done a gap analysis on the basis of the reports and asked banks to bridge the gaps. IB-CART, CERT-IN, NCIIP help Banks in disseminating and foster sharing information associated with physical and cyber events (incidents/threats/ vulnerabilities) and resolution or solutions associated with the bank's critical infrastructures and technologies (Krishna, 2017, Anuraj, 2017). Information Technology Act 2000, and subsequent amendments focused on Digital Signatures, E-Governance, Justice Delivery System, Offences and Penalties. There is a need to enhance the scope and definitions of the Act in the light of ever-changing cyber space and attacks.

Transaction monitoring.

It is observed that cyber heists take longer to detect, and the damage would have happened by the time it is noticed. While focussing on cyber security, banks should not forget to monitor the transactions through FRM (Fraud Risk Management) solutions to identify fraudulent transactions on the fly. Banks should build some scenarios under which fraudulent transactions can take place and build alert mechanism for monitoring such online transactions. The catastrophic effect on cyber security and performance of the banking and financial sectors has made them to take stringent actions on the protections of the security systems in these industries. Transaction monitoring mechanism has given the means to find the clutches of the cyber breach mechanism and cyber-attacks on the customers by identifying the cyber-attacks and crimes zones based on place, time, and frequency of attacks on the security breach of systems and direct customer information KYC assortments.

Emergence in need for online banking innovation:

Unified Integration: Internet-based online Banking has become the need of the hour, to transact efficiently quick seamless banking transactions. Online

Banking systems provide integrated banking operations transactions which eases the demand and supply chain management in all their dealings with oversighted technology.

Reduction in Cost of Operations and Services: The digital information technology has evidently reduced the cost of operations and services provided to customer from traditional banking operations. It uses the operations of automations and Artificial Intelligent software program without human intervention.

Network Connectivity: with the use of internet and technology through proper networks makes the transactions easy and quick anytime and anywhere. Because cost efficient networks provided by the service provider has increased consumption of technology in an economical means.

Surge in Data Accessibility: Especially during Pandemic COVID-19, it has found an increase in data usage and increase in data accessibility and availability, where people began to shift from manual operations to digital methods. This has increased the usage of non-financial operations.

Cloud or Core Banking Technological Infrastructure: Due to the development of cloud or core banking systems in banking operations, has given customer to experience the ease of banking anywhere or in any branch as it acts like a centralized form of operations of transaction for customers daily needs. A core banking system is the centralized back-end software that handles everyday banking transactions for customer's financial records in terms of ledger and account maintenance of the customers data.

Clambering up Banking business operations: As the Indian Financial system is centered on the banking and financial sector functions as they build up the economy. It is very important to improve the technological development in these sectors. It can improve the overall Indian financial sector by providing cloud-based services to the customer and the economy. It helps in scaling up the banking business operations in much more fast and easier way both for the customer and bank if there is technological infrastructural development.

Cyber security and privacy systems in nationalised banks in India.

Cyber Security and Privacy system in Indian Nationalised Banks is a big-time challenge in today's digital era. Cyber space and use of online platforms have increased drastically over years and especially during pandemic in COVID -19 times. There is also a visible surge in cyber- crimes where users and customers are unaware of the facts of being hacked and tracked. Most of the cyber-crimes takes place as the user or customers themselves give information's about their credentials without knowing that they are attacked and cheated on cyber space. As the world is moving towards digitalisation in all the transaction, it has become inevitable that cybercrimes are variably increasing. To protect the security and privacy of the user customer all Banks and Nationalized Banks in India as well as

in the entire globe is trying hard to give a safely and encrypted system of operations. The following are the protection mechanism which is given by banks to prevent and safeguard customers from cybercrime:

Know Your Customer and Know Your Account: The nationalized banks have adopted the policy of updating the information on customer and their account through KYC (Know Your Customer) and KYA (Know Your Account). Banks yearly and if there are any changes in the customers details and account modifications, they are asked to update the form. Though this bank can have complete details and can provide secured service to the customer.

Secure system with up-to-date configuration: Cyber-attacks use different software to attack the computer if it is not up-to-date and configure to the security level. They can access the system through web content and internet downloads. Configuring with up-to-date operating systems can secure the information.

Anti-virus and firewall turned on actively: Installation of Anti-Virus and Firewall in the system can protect the computers from hackers and attackers by blocking and gives notification on the webpages. It protects from harmful threats and steal information of the users.

Set Strong Passwords and PIN: Setting up of strong username, passwords and Personal Identification Number can be a major way of securing the account. In some banks these credentials have an expiry period, and the customers are requested to change the credential often to prevent from hacking. Case and character sensitive credentials are also used to highly secure the accounts from any of the attacks.

Frequent Review Bank Statements and financial statement: One of the most important advice given by the banks is checking banks and financial statements frequently can help the customer to track debit and credit balance and transaction details. This helps the customer to monitor the transaction summary and any malicious transaction and prevention of fraud.

Alerts through SMS and Emails: In almost all the nationalized and other banks this system of SMS and Email alerts has been practiced. If there are any malicious or suspicious logins into the account or money request or withdrawal of money or ATM debit card and Credit card swipes are automatically indicated to the customers through immediate SMS and emails which is connected to bank account. This keeps the customer aware on the transactions details and if there is any suspicion takes place the customer can block and track the account by requesting the bank.

Awareness Programme from Apex and Nationalized Banks: The Reserve Bank of India is called as the Apex bank which guides, advice and monitors the bank system in Indian. It has designed awareness programme on digital frauds, hackers, attackers and protect the customers to secure their accounts credentials. It has instructed all the citizen and customers of the nationalized banks that the

nationalized banks will never ask any customer to reveal information or credentials through indirect source and not to respond to any phone calls, emails, and any form of indirect information collection for PIN, Passwords, CVV or OTPs and the nationalized banks will never collect information through these sources. If any customer information required, they are requested to come to the branch for verification.

Secret Socket Layer used in Banks: This is a back-end web application program which is used as a mandatory protocol to secure the webpage operations by verifying Secret Socket Layers (SSL) certificate. Before accessing and using any webpage the user can either verify the SSL certificate, expiry, and authentication. If the all the provisions are right, then they can use those webpages to browse and feed in credentials for online banking transactions.

OTP, TP, QR: One Time Password (OTP), Transaction Password (TP) and Quick Response Code and Protocol is the most secured form of protecting and preventing the digital frauds and hacking of accounts for money transfers online. Each of these protocols are connected to the mobile number which is registered with the bank account. For any of the transaction related to transfer of money cannot happen without OTP and TP numbers which is sent via encrypted SMS. In QR codes the customer can scan digitally with the encrypted codes and make direct payments with the help of transaction and money request passwords. In India this is the highly secured way of defending the customer and user from digital frauds.

Authenticated Security Questions on transactions: According to Reserve Bank of India advice on multifactor authentication protection based on security questions. For every login or forget password logins this security question authorization is used. This is given by the customer at the time of creation of online bank account. There are three opportunities given to the customer is the security question is answered wrongly and after which account blocking will take place automatically.

Tokens: As part of Multifactor authentication scheme given by Reserve Bank of India, there are three forms of tokens such as USB Token device, Smart Cards and Password-Generating Token are provided for both bank customer and retail customer.

Digital Signature: Electronic or Digital signatures are created in form of authenticated certificate which is used to customer identification and access control on the account for transaction. For any digital payments and transactions, the digital signature should be matched for identification and authentication from any digital frauds.

Research study background.

In the contemporary world with upgrading Technological advancement has not only changed the business operations but also Indian financial sector

through Banking operations. It is benefitting both in terms of qualitative and quantitative manner which has brought development in the country at large. The rapid growth of data operations and sciences has changed the lives of human beings in modifying the standard of living of the people. As banking industry is the base for the Indian financial system it has contributed distinctively to the growth and development of the economy. The adaptation and utilisation of technology in banking operation through automated core banking and cloud banking services has given an upward push to customer online banking (Mistrean, 2023$_a$). At the same time due to growing technological advancement there is also increase in cyber- crimes and digital frauds where customers are cheated unknowingly. The background study focuses and build upon the protection, prevention and awareness of these cyber-crimes and digital payment frauds where customers fall as prey through bogus online banking systems. The study originates from the Indian perspective of study and understanding the banker and customer relationship in online banking services and focuses on the security and prevention of online financial crimes. There is a plenty of scope for the research as it understands and evaluates the bank customer awareness on online banking regarding to cyber security and digital payment fraud prevention particularly in nationalized banks (Mirdul, 2019).

Aims and objectives of the research study:

- to understand the level of awareness among consumers while utilizing the E- banking services;
- to review the recent scenario in cyber- crimes and digital frauds occurring in E-banking services;
- to examine the safety and security mechanism used to protect customers from cybercrimes and frauds;
- to study the preventive measures and safety tips given by nationalized banks for customers against cyber frauds and crimes.

Testing of hypothesis statement:

H1: There is significant difference among consumer's occupation and level of awareness on Laws relating to cyber security and privacy in E- banking;
H2: There is significant association on gender of the consumers on awareness towards cyber- crimes and cyber security systems;
H3: There is significant impact on the age of the consumer towards cyber-crimes and cyber security issues;
H4: There is significant relationship on the income of the consumer and experience on cyber-crimes, security issues;
H5: There is significant relationship on the occupation of the consumer and experience on cyber-crimes, security issues.

2. Literature Review

Esther Ramdinmawii and et al., (2014) cyber-crime studies that there is an increasing monetary damage which is nearly 781.84 million U.S. dollars. The study speaks about the different types of crime committed in today's world. There are many rules and regulations laid down by different laws across the world to prevent the cyber-crime, but it fails when people are not aware of these laws.

K. Mohapatra (2016), Cyber-crimes cases risen from 89% to 94% and the financial losses due to it had also grew from 45% to 63 %. It also revealed that around 70% considered that financial institution was well outfitted to combat cyber fraud.

Maarten Gehem et al., (2015) reports on cyber-attacks are in shortage of number of findings on menace of cyber assessments. Maximum number of reports are focused on large business houses, also states that Research must be conducted focusing on the awareness of cyber-attacks among the public.

Pradeep Mullekyal Devadasan (2015) The researcher highlights the sustainability of Banking sector across the world In this paper the author studies various banking services using information technology and shows the need for cyber security by stating the depth of cyber- crime committed during a period of three years from 2010 to 2013.

Animesh Sarmah and et.al., (2017) Customers are cheated with the prevailing technology, until these people publish their situations even the laws governing cyber-attack will not be saving them. So, it is important that people dealing with money to be careful with their transactions and come forward to stop this criminal act by recording the damages with the Police station. The authors also emphasis that there should be consistent efforts among all the nations with co- operation to act against the cyber-crime.

Jaafar.M.Alghazo and et.al.,(2017) These authors clearly sate in their work that banking using Internet platform is increasing as it is the comfortable way of banking. The increased access of banking using Internet has also increased the threat of cyber security and it is a big challenge for banking sector to protect their customers from cyber-attacks.

KPMG (2017), According to reports the offender's gained access by using spear phishing. In a survey conducted on cybercrime, it has been pre-meant that primarily banks were not well outfitted with adequate cyber security mechanism, because of which they were capitulated to impending cyber threats.

Union Bank of India, (2017) Indian banks have been witnessing persistent attacks from possible state, organized criminals, and hackers. The case of cyber-attack on Canara Bank in the year 2016 explains this better, where bank's e-payments were tried to be blocked by sabotaging its site through the attachment of malicious software. Union Bank of India also fell prey to an attack in July 2017, where close to USD 170 million was looted from its Nostro account.

Burra Butchi Babu (2018) Government's encouragement since demonetisation in November 2016 has brought unprecedented spurt in new digital Banking customers and Digital Payments have registered a record growth. Banks have scrambled to implement various new mobile banking technologies like Wallets, Utility Bill Payments, 24x7 money transfers etc. Lot of mobile applications were developed by banks and most of the new digital users were new to digital banking. This called for greater focus for revamping of cybersecurity in Banks and Financial Institutions.

Hussain Aldawood and Geoffrey Skinner (2018) one of the most straightforward solution for cyber security is through effective training and education programs. As such, in their paper they show the details of how innovative information security education programs can effectively increase user awareness and ultimately reduce cyber security incidents.

Mirdul Sharma and Satvinder Kaur (2019) Cyber-crime has become a menace to the society as majority of people are losing on their data with money to the hackers. The cyber criminals find the easy way to make money out of this updated technology and crack the information through unauthorized access.

Subodh Kesharwani (2019) states that, in the current situation, with the increase in the number of issues related to cyber security there has been increase in the issues connected to the area of digital privacy. Cyber-attacks look as a global threat; hence, organizations need to establish innovative methods in cyber digital world to cater cyber-attacks, focusing mainly on Banking industries.

Gupta Nakul and Jhamb Dharmender (2020) Provides insight into fraud mechanisms, and then addressing loopholes through relevant policy interventions, the paper develops an evolutionary history of fraud and preventive tools to control its various forms. They focus on the need to prioritize interventions, defining those interventions and analyzing their efficacy & potential for change.

3. Research design

This study research design includes both descriptive and exploratory research approach with some empirical background evidence. The study is done to find out the consumer awareness on cyber-crimes, security, and privacy in online banking with reference to nationalized banks. The exploratory research approach is done on the past and existing literature review in formulations of study focused objectives and hypothesis. The descriptive research approach was used to study the theoretical aspects for testing the hypothesis and to conclude the study. The study includes both qualitative and quantitative approach from the data analysis and for concluding interpretation.

This study has collected primary data from the customers based on their awareness of e-banking and related issues. It is a fact-finding inquiry with user

experience with nationalised bank e- banking services. The population characteristics are estimated based on data collected on the survey method.

4. Method of data collection

Based on past literature and research questions both the primary data and secondary data sources were used to collect information pertaining to the research requisites. The Primary data collected through survey method using questionnaire. The questionnaire contains questions relating to the study area on consumer awareness towards cyber-crimes and security/ privacy in Nationalized banks in India.

Data from secondary sources such as research papers, government documents, annual reports, journals, published academic working papers, report findings of RBI, NCRB, NITI Aayog and CERT-IN, data banks from nationalized banks, E- journals, Journal of Banking and Finance etc.

5. Findings of the research study

The key findings of the research are found on the analysis made on the respondent data collected in the research survey based on the awareness of customer towards safety, security and cybercrimes and frauds in online banking in Nationalized Bank in Bengaluru city. The major findings are classified based on demographic profile with study variables undertaken in the study.

The following are the key findings and hypothesis test interpretation of the results.

Findings on classifying 19 sector Nationalized Banks in India, inferring that the highest 44% of the respondents have bank account in SBI, 12.7% of the respondents have account in UCO bank, 6.9% of the respondents have account in Canara bank, 5.9% of the respondents have account in Indian Bank, Indian Overseas Bank and Union Bank of India.

The study finds 80.4 % of the respondents are using Online Banking and 19.6% of the respondent do not use online banking and observed using traditional banking for bank transactions.

It is found that 40.2% of the respondents are already using e-banking services and are aware of the usage, 28.4% of the respondents have started using online banking after suggestions given by family and friends, 21.6% of the respondents are using online banking because of the advice and recommendation given by the bank officials on online banking.

Customer usage of E-Banking Services provided by the Nationalized bank, where 54.9% of the respondent strongly agree, 24.5% of the respondents agree on the usage of the E-Banking services and majority of the respondents are convenient using them. 31.4% of the respondents use online banking for personal transactions, 25% of the respondents use for online transfer of money

(NEFT/RTGS), 20% of the respondents use paying all bill transactions, 13% of the respondents use for regular banking transactions and 11% of the respondents use for online shopping purposes. It is found that, 35.3% of the respondents always use online banking for every usage, 29% of the respondents use online banking occasionally, 16.7% of the respondents use online banking for every transaction and the remaining 18.7% of the respondents use sometime or never use online banking.

The study results show, 47.1% of the respondents strongly agree on cashless transactions, 36.3 % of the respondents agree on the preference, 12.7% of the respondents are neutral on the either to use nor to prefer, 3.9% of the respondents strongly disagree on the cashless usage and prefer traditional methods of banking.

The results projects that, consumer perception on digitalization of banking services will increase digital fraud and cybercrimes as 40.2% of the respondents agree that digitalization increases frauds and cybercrimes 20.3% of the respondents agree on the same facts, 30.4% of the respondent are neutral neither to agree nor disagree, 7.8% and 1.0% of the respondents think that digitalization in banking services will not increase in the fraud and cybercrimes.

40.2% of the respondent's state that immediate notification sent from bank in case of problem with transactions. 23.5% of the respondents say that notifications regarding the logins to the bank account are indicated to them as a part of security, 18.6% of the respondents say that transparency of the transaction means security for them, 11.8% state that availability of an option to block account in case of misappropriation should be made. 5.9% of the respondents say easy transfer of money without a complicated process should be made for accessibility.

The results illustrate the importance of online banking in banking transaction as 86.3% of the respondents say that digitalization of banking services is very important in today's world for all financial transactions.13.7% of the respondents say they don't feel the importance of online banking in banking transaction.

The results show, the ease of the respondents using online banking for all their financial transaction. 89.2% of the respondents say they feel online banking ease and 10.8% of the respondents say they are not comfortable with online banking. The technology and systems used in online banking are up to date according to the customer's experience. 63.7% of the respondents feel that the technology and systems used in online banking service is up to date. 36.3% of the respondents feel it is not updated according to the technological changes.

The findings exemplify the comparison of using online banking and traditional banking as customers convenience over the other. 91.2% of the respondents feel that online banking is more convenient and easier to use compared to traditional manual banking. 8.8% of the respondents feel that they are

convenient with the traditional banking system. The study represents that 25.5% of the respondents use mobile banking, 23.5% of the respondents use Online banking, 21.6% of the respondents use UPI based transaction,20.6 % of the respondents use debit/ credit card transactions and less than 8.8% of the respondents use traditional banking for their banking transaction. Majority 70.6% of the respondents haven't faced any cyber related issues in online banking. 29.4% of the respondents have faced some form of cyber issues in online banking.

The results shows that customer experience relating to cyber issues in Online Banking, 15.7% of the respondents faced issues with online email frauds, 7.8% of the respondents have faced financial crimes and online money request, 19.6% of the respondents have got phone calls requesting information of their details, 2% of the respondents took data survey for account details unknowing the cyber frauds, 5.9% of the respondents have faced denial of transactions and re-login of pages, 3.9% of the respondents have faced issues on money deducted twice for single transaction and no refund of debited money from the bank and majority of the customers haven't faced any cyber related issued of the above mentioned and are very comfortable with their online banking services.

From the study it is found that customer awareness on banking security system and terms, 78.4% of the majority respondents are aware of Pin authentication, OTP, and UPI payment request. 17.6% of the respondents are aware of the One Time Password (OTP), 2.9% of the respondents are aware about pin authentication and 1% of the respondents are aware of UPI payment request. 51% of the respondents are aware on cyber security laws relating to online banking frauds and cyber-crimes and 49% of the respondents are not aware on the cyber security laws relating to cyber-crimes on online banking.

The result states that majority 86.3% of the respondents' experiences security and safety provided by their banks regarding their account holding. 13.7% of the respondents say that there is no safety and security provided by their bank regarding to their account. The findings show, 62.7% of the respondents feel that banks address the issues relating to cybercrimes regarding online banking. 37.3% of the respondent feel that banks do not address the issues relating to cybercrimes regarding online banking.

The study exhibits that what is most prominent advantage in using online banking in comparison to traditional banking. 32.4% of the respondents feel that online banking is more convenient and fast compared to traditional banking, 27.5% of the respondents feel that it is time effective, 18.6% of the respondents feel that it is user friendly and quick in transaction, 14.7% of the respondents feel that online banking provides varieties of services at one roof, 6.9% of the respondents feel that is safer to use online banking.

The outcomes states, kind of Cyber securities and fraud prevention are provided by your Bank are provided as opinions from the respondents. The

highest 58.8% of the respondents state that providing OTP for transactions prevents cybercrimes and fraud prevention in online banking, 31.4% of the respondents feel that providing SMS for each transaction are safe, 2% of the respondents states that yearly updating on KYC and awareness programs on cybercrimes and online frauds can provided regularly, 5.9% of the respondents feel technological updates and layers of protection can secure their account details and prevent cyber frauds and crimes.

It is found that, 38.2% of the respondents opted neutral option on their opinion that internet is secure for conducting financial transaction. 34.3% of the respondent agree that interest is secure for conducting financial transaction, 15.7% of the respondents strongly agree on the same. Less than 11% of the respondent disagree that internet is not secure for conducting financial transaction. The studied data projects that 49% of the respondents agree that customer services and account details of the recorded transactions are kept accurate and confidential, 26.5% of the respondents neither feel agreed nor disagree on the given statement, 19% of the respondents strongly agree on the given statement, less than 4.9% of the respondents disagree on the given statement.

The result of findings shows that 30.4% of the respondents feel that online banking is more convenient, 28.4 % of the respondents feel UPI based transaction is convenient, 23.5% of the respondents feel that mobile banking is ease and convenient, 11.8% of the respondent feel card transaction is convenient, 5.9% of the respondent feel that traditional banking operations are easy and convenient. Issues relating to customers online blocked payments that are solved by the banks show that, 46.1% of the respondent say yes on the given statement, 10.8% of the respondent feel banks don't clear issues relating to online block payments, 40.2% of the respondents say that there is delay in processing the issues relating to clearing blocked payments, 2.9% of the respondents say that the banks solve the issues relating to blocked payments online.

The findings states that 59.8% of the respondents feel that nationalised bank provide safety, security and quick in online banking, 34.3% of the respondents feel that private sector bank provide safety, security, and quick online banking, 4.9% of the respondent feel foreign banks provide proper service, 1% of the respondents feel that RRB provide service on safety, security and quick in online banking. The outcome shows that 57.8% of the respondents are satisfied with the services provided by banks, 18.6% of the respondents feel that they are highly satisfied with the online banks' services, 17.6% of the respondents feel neutral, 3.9% of the respondents feel dissatisfied and 2% of the respondents feel that they are highly dissatisfied with the online service offered by their banks.

Results of Hypothesis testing based on Chi- Square test and Pearson's Correlation test on demographic profile of the respondents with the study variables are listed below:

The hypothesis test result of Pearson's Chi-Square analysis show, the p value is greater than the selected significance level alpha=0.05, we accept the null hypothesis and reject the alternative hypothesis stating that there is no significant difference among consumer's occupation and level of awareness on Laws relating to cyber security and privacy in E-banking.

The hypothesis test result of Pearson's Chi-Square analysis show, the p value is greater than the selected significance level alpha=0.05, we accept the null hypothesis and reject the alternative hypothesis stating that there is no significant difference among consumers on awareness towards cyber-crimes and cyber security systems and gender of the respondents.

The hypothesis test result of Pearson's Chi-Square analysis show, significant impact on the age of the consumer towards cyber-crimes and cyber security issues (N=102). The analysis showed that there was significant evidence to accept the null hypothesis and conclude that there is a weak negative impact between age and cyber security issues in online banking. r=-0.22, p<0.01 indicates that there is no and negative correlation between age and cyber-crimes issues.

The hypothesis test result of Pearson's Correlation coefficient analysis shows no significant relationship on the income of the consumer and experience on cyber- crimes, security issues (N=102). The analysis showed that there was significant evidence to accept the null hypothesis and conclude that there is a moderate negative impact between income and cyber security issues in online banking. r=-0.72, p<0.01 indicates that there is no and negative correlation between income and experience on cyber-crimes issues.

The hypothesis test result of Pearson's Correlation coefficient analysis shows the evaluated no significant relationship on the income of the consumer and experience on cyber-crimes, security issues (N=102). The analysis showed that there was significant evidence to accept the null hypothesis and conclude that there is a low positive impact between income and cyber security issues in online banking. r=0.110, p<0.01 indicates that there is no correlation between occupation and experience on cyber-crimes issues.

6. Suggestions and Recommendation

Based on the findings from the research study, the following suggestions and recommendations are drawn in aspect of customer awareness towards Cyber Security and Digital Payment Fraud Prevention in Nationalized Banks. The customers should check and verify any of the information asked by the external sources while using online banking before transacting. Never share any information relating to personal data such as name, date of birth, PIN, card details to anyone especially while feeding data in any online platforms for transaction in e-retailing through online banking. customers can monitor their bank account regularly by checking the bank statements both online and book mini statements.

Verifying the webpage security settings and secured pages before logins. As directed by the RBI, no banks make call to any customer for information verification on KYC and getting their account and card related details, so they should never share information through phone calls.

In the case of banks, they can provide a real time solution through help lines and 24X 7 hot lines to the customers for any problems faced by customers in online banking. updating and security checks in technology used in banks for user friendly secure online banking services to customer. Anti-cybercrimes policy and technical professional support can be implemented by the banks to secure customers from any fraudulent activities by the hackers. Quick response and detection of online frauds technological solutions can be implemented and digital certification on the site information can be provided by the banks.

7. Conclusion

In the past two decades there has been tremendous growth in information and technology which has given way to innovation in all sectors of business. This has greatly brought changes in the financial sectors as it is the base for any business operations. In the banking sector these financial innovations and technological developments have made the customer to do easy of transactions for every financial and retail requirement.

As developments are made in technology this has even given development in banking operations. Despite various technological developments offered to end customers by providing electronic banking services, it has also given some critical drawbacks in terms of complete security and privacy to online bank users. In the current scenario it has become like a basic necessity as more and more customers use online banking services in operating bank account for various purposes and for financial needs. As the apex bank, Reserve Bank of India has been giving directions to all banks and exclusively to all nationalized banks about cyber security and cyber protection from any online frauds in all moments in time, by creating awareness on cyber security, protection, hacking and other cyber frauds where customers are unknowingly cheated and fall as prey to all kinds of online frauds.

Therefore, this research project attempts to seek and analyze customer's awareness on cyber security and digital payment fraud prevention in nationalized banks based on the respondents view on e-banking services. According to the result analysis, it was identified that customers who ever uses online services for retail and banking services irrespective of age, occupation, income, gender, education level they are vulnerable to online frauds if they are instinctive towards online frauds, anonymous calls and hacking of information. There is no significant difference on the study variables with demographic profiles. Similarly, the outcome shows that customers are aware about all online products of e-

banking services, aware about cybercrimes and less aware bout the laws relating to cyber protection while using e- banking services.

Thus, the analysis and findings of the study was useful to understand consumer awareness and variable factors that has determined their insight about their security, privacy and cybercrime protection while using online banking services.

References

Aithal, P. (2015). Recommendations on Policy & Regulatory Guidelines for Mobile Banking In India. *International Journal of Management, IT and Engineering (IJMIE),* Volume 5, Issue 7, 1-20.

Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017). The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services. *Int. J. e-Education, eBusiness, e-Managemente-Learning*, vol. 7, no. 1, 70–78.

Animesh, S. et al. (2017). A Brief Study on Cyber Crime and Cyber Law's of India. International Research Journal of Engineering and Technology (IRJET), vol.4, no. 6, 2017, pp. 1633 -1640.

Anuraj S. (2017). Studies Report on Cyber Law in India & Cybercrime Security. *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 5, Issue 6, 7-26.

KPMG. (2017). Cybercrime Survey Report - Assets. kpmg.assets.kpmg/content/dam/kpmg/in/pd f/2017/12/Cyber-Crime-Survey.pdf.

Krishna K., Praveen G. (2017). A brief study on Cyber Crime and Cyber Law's of India, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06 |June -2017, 43-56.

Krishna P. and Aithal, P. (2017). Mobile System For Customized And Ubiquitous Learning By 4G/5G. *International Journal of Management, IT and Engineering (IJMIE*), Volume 5, Issue 7, 63-71.

Lakshmanan, A. (2019). Literature review on Cyber Crimes and its Prevention Mechanisms: *ResearchGate*, 1–5.

Mistrean, L. (2023$_a$). Contemporary directions on how consumers interact with financial-banking services. *The USV Annals of Economics and Public Administration*, Vol 23, No 1(37), 151-161.

Mistrean, L. (2023$_b$). Behavioural evolution of consumers of banking services in the COVID-19 pandemic situation. *Journal of Corporate Governance, Insurance, and Risk Management (JCGIRM),* v. 8, s. 1, 84-100.

Mistrean, L. (2021$_a$). Customer orientation as a basic principle in the contemporary activity of the bank. *Journal of Public Administration*, 21/2021, 39-51.

Mistrean, L. (2021_b). Banking customer relationship management under the impact of new information technologies. *Современный менеджмент: проблемы и перспективы. Санкт-Петербург: Государственный Экономический Университет*, 483-490.

Mistrean, L. (2023_c). Factors Influencing Customer Loyalty in the Retail Banking Sector: A Study of Financial-Banking Services in the Republic of Moldova. *Opportunities and Challenges in Sustainability*, 2(2), 81-9.

Mistrean, L. and Staver, L. (2021_a). Financial literacy and consumer behavior of financial-banking services. *Шестая международная научная конференция: Ростов-на-Дону: Южный федеральный университе*, 82-96.

Mistrean, L. and Staver, L. (2021_b). The impact of COVID-19 pandemic crisis on demand for financial-banking services. 30th Anniversary of the establishment of the Academy of Economic Studies of Moldova". International Scientific Conference, 415-427.

Mirdul S. and Satvinder K. (2019). Cyber Crimes Becoming Threat to Cyber Security. *Forensic Sciences*, Volume 02, Issue 01, 36 -40.

Mohapatra, K. (2016). Effective operational risk management. Cybersecurity vulnerability in Indian banks. *CYBERSECURITY Framew. BANKS*, [Online]. Available: https://financialit.net/sites/ default/file s/customerxps_white_paper_cyber,secu rity_vulnerability_in_indian_banks_1.pdf.

More, M., Jadhav, P. and Nalawade, K. (2016). Online Banking and Cyber Attacks: The Current Scenario. *ResearchGate*, 5. 743-749.

Pradeep, M. (2016). Impact Of Information Technology In Banking- Cyber Law And Cyber Security In India. *International Journal of Management, IT and Engineering (IJMIE*), Volume 5, Issue 7, 411-428.

Report of The Reserve Bank of India. (2016). Guidelines on Cyber Security Framework vide circular DBS. DeloitteLtd/content/dam/Deloitte/in/Documents/finance/in-fa-banking-fraud survey.pdf.

The Reserve Bank of India (2016). guidelines on Cyber Security Framework videcircular DBS.CO/CSITE/BC.11/33.01.001/2015-16.

Stiawan, D., Idris, M., Abdullah, A., Aljaber, F. and Budiarto, R. (2017). Cyberattack penetration test and vulnerability analysis. *Int. J. Online Eng.*, *vol*. 13, no. 1, 125–132.

Sravanthi G. (2016). Fraud & Risk Management in Digital Payments. *International Journal of Recent Research Aspects*, Vol. 3, Issue 3, 38-44.