

**ROLE OF INTERNET BANKING IN FRAUD AND IDENTITY
THEFT IN HIGH-POPULATION COUNTRIES: A CASE
STUDY OF INDIA**

Name : Hardikkumar Hareshbhai Solanki

Student id: 2220271

Supervisor: Jia Miao



Master's Degrees by Examination and Dissertation

Declaration Form.

1. This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed: Hardikkumar Hareshbhai Solanki

Date: 11/02/2024

2. This dissertation is being submitted in partial fulfilment of the requirements for the degree of Master in Business Administration.

Signed: Hardikkumar Hareshbhai Solanki

Date: 11/02/2024

3. This dissertation is the result of my own independent work/investigation, except where otherwise stated.

Other sources are acknowledged by footnotes giving explicit references.

A bibliography is appended.

Signed candidate: Hardikkumar Hareshbhai Solanki

Date: 11/02/2024

4. I hereby give consent for my dissertation, if accepted, to be available for photocopying, inter-library loan, and for deposit in the University's digital repository

Signed (candidate): Hardikkumar Hareshbhai Solanki

Date: 11/02/2024

Supervisor's Declaration.

I am satisfied that this work is the result of the student's own efforts.

Signed: Jia Miao

Date: 11/02/2024

Table of Contents

Chapter 1	6
1.1 Introduction.....	6
1.2 Background and context to the study	6
1.3 Research aim, questions and objectives	7
1.4 Significance of the study.....	8
1.5 Carrying out the research and Research Limitation	8
1.6 Structure of the dissertation.....	10
Chapter 2: Literature Review	11
2.1 Introduction.....	11
2.2 Overview of internet banking in India	11
2.3 Security metrics for Internet banking.....	14
2.4 Type of Internet Banking Fraudulent Activities in India.....	15
2.5 Impact of such fraudulent activities on customers	16
2.6 Regulatory Framework for Banking Services in India.....	17
2.7 Technological and Innovative Solution.....	18
2.8 Awareness and education level of customers regarding such fraudulent activities	19
2.9 Challenges in Internet Banking.....	20
2.10 Internet Banking Fraudulent Activities Cases in India	21
2.11 Literature gap	22
2.12 Summary	23

Chapter 3: Research Methodology.....	24
3.1 Introduction.....	24
3.2 Research philosophy	24
3.3 Research approach.....	26
3.4 Research design.....	29
3.5 Research Strategy.....	31
3.6 Data collection tools and methods	31
3.7 Data analysis	32
3.8 Ethical Consideration	32
3.9 Research limitation.....	33
3.10 Research Timeline	33
3.11 Summary	33
Chapter 4. Data Analysis and Findings.....	34
4.1 Introduction.....	34
4.2 Quantitative Data Analysis.....	35
4.4 Discussion and Findings.....	60
4.5 Conclusion.....	64
Chapter 5. Conclusion and Recommendation.....	65
5.1 Summary	65
5.2 Linking objectives with the study	66
5.3 Recommendation.....	67
5.4 Limitations of Study.....	68
5.5 Future Scope of Study.....	68
References.....	70
Appendix.....	76

Chapter 1

1.1 Introduction

In this era of technological development and changes, financial technology has also observed rapid advancements. In this context, it is found that the prevalent adoption of online banking has been accompanied by unparalleled convenience as well as accessibility for managing individual finances. Countries with higher populations have a huge base of consumers that stand at the front of this significant revolution of digitalisation. Jibril et al. (2020) argued that online banking has significantly changed the conventional way of carrying out banking practices. At the same time, various novel challenges have been identified, mainly in the context of fraud as well as identity theft. This present study aims to conduct an in-depth study on the multi-dimensional role of online banking which has a significant contribution to several instances of identity theft as well as fraudulent activities, with respect to India.

1.2 Background and context to the study

An increase in the use of internet-based financial transactions in highly populated countries has made these countries an attractive and easy target for cyber-attackers looking to exploit the weaknesses present in the online systems of banking (Tajpour and Zamani 2020). This present study seeks to investigate various aspects of this particular phenomenon while researching the strategies implemented by cyber-attackers, the weaknesses present in the infrastructure of online banking, as well as the influence on a wide base of users within these highly populated countries.

Phishing attacks as well as social engineering cons have become a universal technique in the arena where cyber-attackers target the users of internet banking. Therefore, Ali (2019) opined that it further necessitates an in-depth understanding of the psychological as well as technological factors that has a significant contribution to the success of such deceptive activities. Further, Ibrahim (2019) added that as development in technology takes place, so does the complexity as well as the superiority of cyber-attacks. This study also explores various trends present in the field of cyber-attacks, which also includes the implementation of high-end malware as well as ransomware, along with the impact of these cyber-attacks on the security of internet banking, with respect to highly populated country, India.

The incorporation of smartphones into the financial ecosystem also provides a lot of convenience but at the same time, it also generates a lot of new threats to the users (Nwarize 2023). Hence, this study focuses on various risks that are related to mobile banking with respect to India and further recommends certain strategies that can help improve the security of these platforms. Apart from these, Mawgoud and Ali (2020, February) stated that the regulations governing the online banking systems in these highly populated countries also have an important role to play as they shape the security landscape of the financial industry. This study also examines the current regulations, determines potential loopholes, and recommends suggestions for enhancing the regulations, which helps ensure that the regulatory framework remains vigorous as well as adaptive to the developing landscape of risks.

On an overall basis, this study focuses on offering an in-depth analysis of a complicated interrelationship shared between online banking, fraudulent activities, as well as identity theft with respect to India. By giving utmost importance to the challenges as well as suggesting certain solutions, this study further aims to provide a significant contribution to the constant discussion on preserving the honesty as well as security of digital financial ecosystems in highly populated countries.

1.3 Research aim, questions and objectives

The main aim of this study is to assess the impact of Internet banking on fraudulent activities and identity theft with respect to densely populated countries. With respect to this aim, the researcher has prepared the following objectives for this study that help in accomplishing the overall purpose of the study.

The questions of this study are:

- What are the strategies implemented by cyber-attackers in India?
- What is the impact of cyber threats on psychological as well as behavioural aspects of individuals in India?
- What are the risks linked with mobile banking and online banking?

The objectives of this study are as follows:

- To inspect the strategies implemented by cyber-attackers in India

- To find out the impact of cyber threats on psychological as well as behavioural aspects of individuals in India
- To find out the risks linked with mobile banking and online banking

1.4 Significance of the study

This study has a lot of significance as it provides thoughtful insights into the complex interrelation between online banking and fraudulent activities, especially when highly populated countries are concerned. There are various reasons that make this study significant. First, it offers a precise understanding of the developing landscape of threats to financial institutions as well as technology providers. Further, this study is also important for policymakers as well as regulatory bodies. This study can provide a significant contribution in developing stricter as well as adaptive regulations by examining regulatory frameworks. According to Reynolds (2022), better and enhanced regulatory frameworks act as a warning to cyber-attackers and help the organisation to have a safe and secure ecosystem.

This study also explores the impact on users as well as the assessment of awareness of cybersecurity, which helps in providing crucial information to educational institutions. In this regard, Shaaban (2020) stated that financial literacy programs can be implemented to address such threats and adopt safe and secure online practices. The importance of this study is further extended to an international community because the findings are related to India, which is one of the highly-populated countries, and findings from the study resonate with other highly-populated countries that may have a significant impact on global practices of cybersecurity. On an overall basis, it can be said that this study has a significant potential to contribute to academic knowledge along with practical implications that can help enhance the security, inclusivity as well as resilience of online banking in highly populated countries.

1.5 Carrying out the research and Research Limitation

Carrying out the research

In order to find answers to this dissertation's issues, the researcher will choose a primary approach and collect direct basic evidence and facts. These will then be examined and compiled. This study intends to employ a quantitative approach to acquire primary information. Additionally, a survey questionnaire will be administered to the sixty responders who are banking clients. After that, the gathered data will be represented graphically by the scholar

when they carry out statistical data assessment. Moreover, to guaranteeing that helpful details is derived to make useful conclusions from this present dissertation, graphical depiction of the details exhibits as well as clarifies survey respondents' answers.

Research Limitation

The increase in online banking services in highly populated countries has indisputably changed the entire landscape of financial services which has offered extraordinary convenience as well as accessibility. However, this digital transformation has a lot of challenges, such as the dominance of fraudulent activities as well as identity theft with respect to online banking that poses a significant threat. Despite such development in the field of technology as well as security metrics, the increasing frequency as well as complexity of cyber-attacks within highly populous countries leads to major concerns.

The main problem of this study is the ineffectively addressed threats as well as vulnerabilities related to online banking, particularly emphasising the increased experience of users in highly populated countries. It is opined by Tick et al. (2021), that the significant amount of online transactions, combined with developing cyber-attack risks as well as diverse demographics leads to a multifaceted landscape where fraud flourishes. Various fraudulent activities and the implementation of cyber vulnerability have become universal issues while misusing the varied base of users in densely populated countries. Mobile banking is one of the most popular resorts for carrying out financial transactions, and at the same time, it brings in new realms of exploitation, which requires a comprehensive understanding of the related risks as well as effective strategies for mitigating these risks.

A lack of proper awareness about cybersecurity among the users, along with potential gaps present in the regulatory framework, further worsens the challenge. The current state of these regulatory frameworks raises crucial questions regarding the competence of current security aspects, their effectiveness and the need for customised strategies that help in addressing the distinctive aspects of online banking with respect to highly populated countries. This study further tries to address these major concerns by carrying out an in-depth analysis of multilayered issues of fraudulent activities as well as identity theft with respect to online banking in India. Finding out the main reasons, evaluating the impact on wide user groups, and recommending appropriate solutions, this study helps contribute important information on the current efforts for securing the financial landscape in countries with high populations.

1.6 Structure of the dissertation

The structure that is followed in this study is as follows:

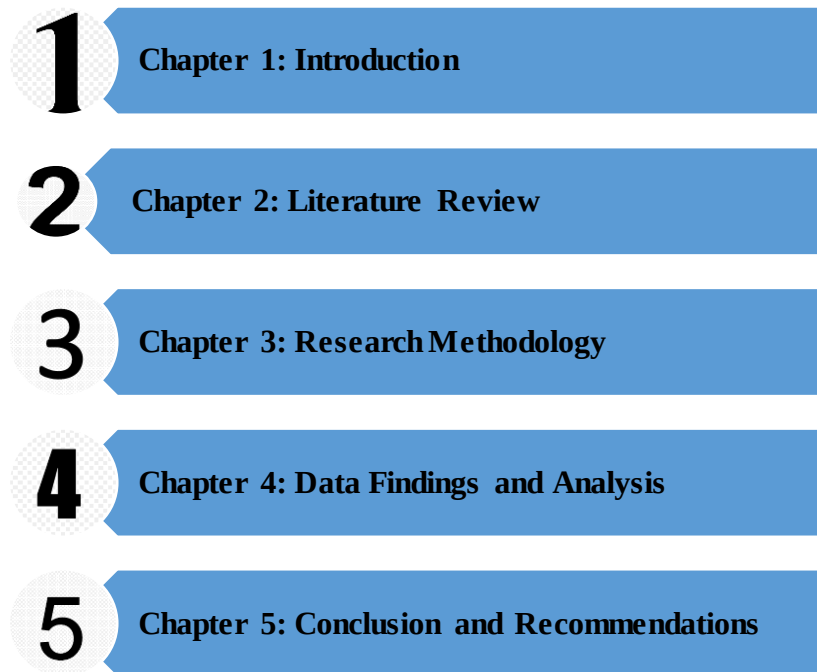


Figure 1: Structure of the dissertation

(Source: Created by the researcher)

Chapter 2: Literature Review

2.1 Introduction

The development of internet banking has changed the entire landscape of financial services that are being carried out in India. It offers unparalleled ease as well as accessibility to the users. However, this development is complemented by a growing concern, which is increasing incidents of fraudulent activities and identity theft within the arena of internet banking. This present review aims to provide an in-depth analysis of the multilayered role that is played by internet banking in enabling as well as battling against fraud as well as identity theft with respect to the financial sector of India. All this information is presented in this current chapter, which is referred to as a literature review. It is one of the most crucial chapters in a dissertation, which provides an in-depth understanding of the research topic. According to Kaur and Arora (2020), it is a process of summarising the current research as well as scholarly articles and other major sources that are associated with the current research topic. In this present chapter, various sub-heads regarding Internet banking and fraudulent activities are prepared as well as analysed in detail, which further helps in carrying out an effective and sound study.

2.2 Overview of internet banking in India

Internet banking is referred to as online banking and sometimes it is also called e-banking, and net banking. According to Manoj (2021), internet banking is defined as the facility provided by banks and other financial institutions that help customers to utilise banking services through the internet. Therefore, customers who use internet banking the customers are not required to visit the bank to avail of any sort of service. However, Jibril et al. (2020) stated that in India, not all account holders can use the services of internet banking. Hence, in order to use these services, it is required for the customers to register themselves while opening their accounts in the bank or later.

Private and foreign banks were the first to introduce internet banking, and public sector banks soon followed. The Reserve Bank of India (RBI) identified the potential of mobile banking in October 2008 and released the first set of rules. As to the standards, mobile banking refers to the utilisation of mobile phones by bank customers to conduct financial transactions, which may involve credit and debit of their accounts (Verma and Kumar, 2020). In an effort to improve customer confidence and keep pace with technological advancements, the RBI has

mandated that all transactions, regardless of amount, be correctly encoded. In this regard, Vig et al. (2022) opined that mobile banking services are mainly available through Toll-free numbers with the help of SMS, GPRS, USSD or mobile applications.

Growth:

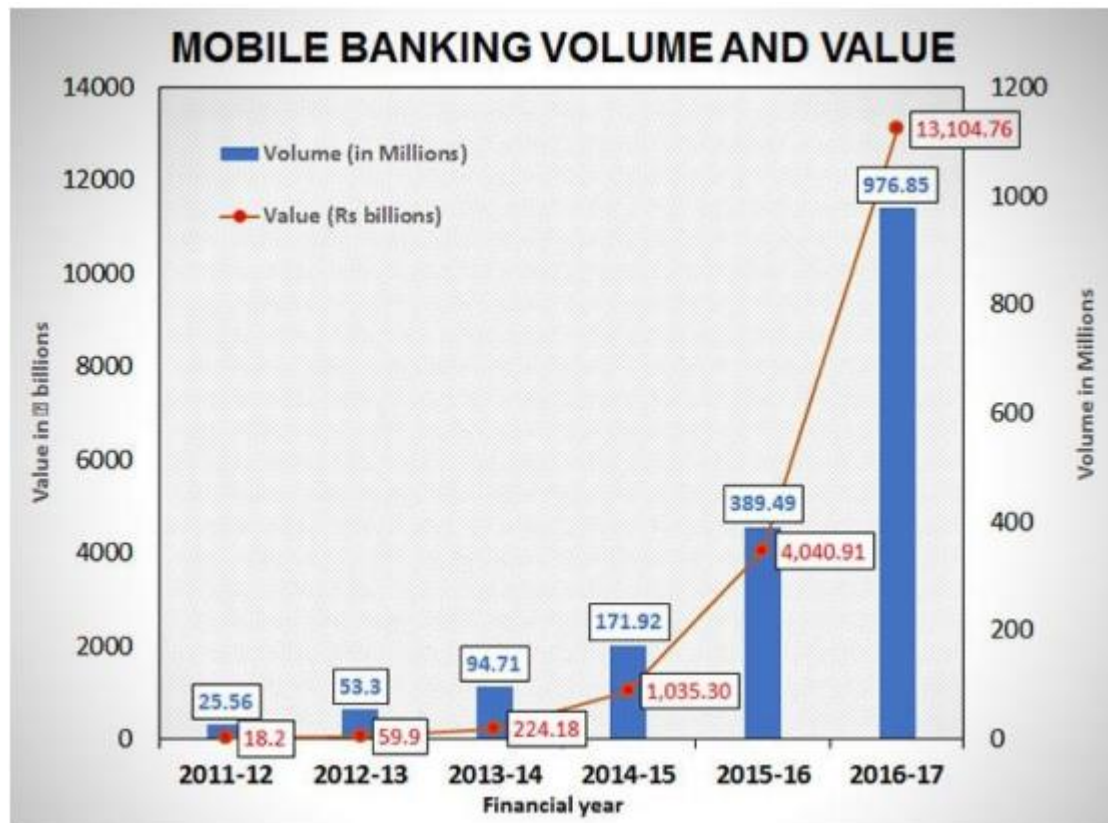


Figure 2.1: Mobile banking and its growth

(Source: KOTTECHA, 2019)

According to the graph stated above, it can be said that this graph demonstrates the usage of mobile banking in India. According to this graph, the usage of Internet banking is demonstrating a positive trend in the year 2010-11 to 2016-17. It is also found that the number of transactions has also increased for the given period, with respect to the transaction value, it is found that it was INR 25.56 million in the year 2011-12, and a significant growth of 150% in terms of volume, as well as 224% in terms of transaction value, is observed during the financial year 2015-16 to 2016-17 (KOTTECHA, 2019).

With the help of Internet services, customers can easily manage their accounts, carry out transactions, and make payments for bills from their comfort. It is further opined by Shaw and

Saha (2020) that the implementation of digital payment systems such as Unified Payments Interface (UPI) has further increased this trend, which helps in carrying out seamless as well as quick methods for transferring funds. Vishnuvardhan et al. (2020) stated that the financial institutions as well as banks in this country, India, have been hasty in embracing technology, providing user-friendly experiences, vigorous security metrics as well as integrated mobile banking applications. RBI has also provided a regulatory framework, which plays a crucial role in ensuring the safety as well as reliability of online banking services (Sarjiyus et al. 2019). Hence, the growth of internet banking services in this country not only demonstrates the changing tastes as well as preferences of customers but also determines the journey of a nation towards an inclusive and efficient digital ecosystem in the financial landscape.

Concerns:

On the basis of the above part of this review, it has been identified that internet banking services have increased a lot in India. However, it has also been found that digitalisation in the field of the financial industry has also observed a lot of major concerns. In order to guarantee the dependability, stability, and credibility of the nation's entire financial system, these issues demand serious consideration (Acharya and Joshi, 2020). Since there are more online transactions, there is also a greater chance of cyberthreats including virus attacks, phishing scams, and identity theft. For this reason, cyber security is one of the most important issues. Consequently, banks need to continuously invest in a robust cybersecurity ecosystem in order to protect client data and financial transactions from unauthorised access and malicious activity.

The need for better user awareness as well as digital literacy is another major concern with respect to Internet banking. In this regard, Dey (2019) stated that the younger generation in this country is more skilful in terms of using the services of internet banking. However, there is still a substantial section of this population in rural areas that does not have proper knowledge as well as skills (Ghosh, 2021). Operational elasticity is another major concern because it may create issues during system failure or technical problems. Therefore, in this regard, Datta et al. (2020, June) stated that online banking services should be highly dependable to avoid disruption while carrying out financial transactions. In addition, Banu et al. (2019) added that banks are required to make significant investments in a vigorous ecosystem of IT, implement effective recovery plans from disasters and carry out regular audits of the system for identifying and addressing vulnerabilities.

Apart from this, privacy is another major concern which comes with the question of handling customer data and identifying whether the data is vulnerable to unauthorised access. It is important to maintain an efficient balance between innovation and regulatory standards compliance (Divya, 2019). However, it is an important challenge. Thus, in this regard, it is required to implement adaptable regulations that are associated with technological developments while saving the interests of consumers as well as the financial system is important to maintain the integrity of internet banking services in India.

Hence, on an overall basis, it can be said that addressing issues of cybersecurity, increasing the awareness of users, ensuring operational flexibility, protecting privacy, and directing regulatory challenges are important factors that can help in addressing the concerns of the Internet banking system in India. A focused effort from banks, regulators, and the government is important for creating a secure as well as resilient digital financial ecosystem that provides significant benefits to all customers.

2.3 Security metrics for Internet banking

As the usage of Internet banking increases, there are high risks of fraud and security measures. For better security approaches, the evaluation of security metrics is effective nowadays. To implement better security systems in their banking, the banks utilize various keys of security metrics. At first, they can track every login number whether it is successful or not. This helps to detect unprotected logins and present valuable data on customer history (Lin et al., 2020). On the other hand, the tracking system also prevents the risk of fraud while customers access their bank accounts. Also, the average response time is one of the useful security metrics in the Internet banking system. It shows the approximate time of banking systems for detecting malware and threats. Proper analysis and focus on encryption can provide effective results to secure customer data. However, accurate tracking of security threats can set a standard for customer data protection.

Banks can use analysis to improve the necessary sectors and adjust for any negative effects. Additionally, banks want to enlighten their clientele about the Internet banking platform. Campaigns, awareness initiatives, training courses, and many other methods can be used to achieve this (Singh, 2019). The dangers of unwanted access must be decreased by educating customers about internet banking. All things considered, the security metrics assist the banks

in keeping an eye on systemic issues and possible enhancements. Additionally, the strong measures improve the user experience for customers in the online banking system.

2.4 Type of Internet Banking Fraudulent Activities in India

In the last few years, India has seen rapid growth in the Internet banking system, which led to various fraud cases on customers. All the fraudulent activities have several types such as phishing, detecting theft, and other high-risk frauds. Some of the common types can be seen in India, such as:

a) Phishing: It is a process of fraud used by criminals to reveal personal information of customer's bank accounts by tricks. From some authentic sources, fraudsters send fake messages that have directions to click on some links (Manoharan et al., 2022). After that, all the personal information of customers was unknowingly revealed to the fraudsters.

b) Smishing: It is one of the variants of phishing that is done by sending messages instead of mail by fraudsters. Through modern technologies, fraudsters create links that are sent to the customers and they easily access financial information through links.

c) Vishing: It is also a variant of phishing that is done by making phone calls to customers. Fraudsters pretend as bank staff and collect information by conversation such as account number, identification details, PIN, and others (Bhatnagar and Mishra, 2019). They also create a scenario of new urgent services by showing fake issues and false cases of fraud with accounts to the customers.

d) Detection of theft: It appears when a customer faces a fraud case with a number, address, and DOB by their name. All this information is used for loans, new accounts, and transactions without the permission of the customer.

e) Skimming of cards: This is done via a small piece of equipment that captures details of the magnetic portion on credit or debit cards (Rouge et al., 2020). Criminals apply these tools to ATMs to collect more card information. It is used for false transactions and creating duplicate cards.

f) Virus and malware attacks: Some viruses, fake security software, and other features are used in mobile and computer devices. After installation of these things, it starts to collect sensitive

information and easy access to secure sites from that device. In Internet banking, all this information helps the fraudsters in more crimes.

g) SIM fraud: It happens when a criminal accesses through the victim's phone number on another device (Gupta et al., 2023). In this incident, they easily receive account-related messages in that number regarding the Internet banking system.

The banks need to adopt new advanced security measures to avoid fraud activities. Implementing protected methods with updated software, monitoring information regularly and other practices can improve the efficiency of Internet banking for customers. Overall, India faces various complexities regarding fraud cases, and appropriate measures must be taken for customer safety.

2.5 Impact of such fraudulent activities on customers

In India, fraud regarding Internet banking has become a vital issue for financial status, safety, and security. Various negative impacts can be seen on customers through fraudulent activities, such as:

a) Financial Loss: The main impact of fraud via Internet banking is financial. Through illegal access to customer accounts, fraudsters can do monetary transactions and hamper the account without the permission of the customers (Leonardo et al., 2021). Sometimes these criminals also use previously stolen information for high-value frauds that can harm customers' financial status.

b) Theft of identification: All these fraud activities can destroy customer accounts and via identification theft, the customer can face a huge impact on credit score. Through this identification, fraudsters can apply for loans, and create new accounts in customer's names. It can create several difficulties for customers such as unknown debts, loans, and bad credit scores.

c) Emotional loss: Sometimes fraud cases can cause emotional loss in customers as they face stress over the leakage of personal information and financial trauma. Also, the loss recovery process is hectic and time-consuming for customers (SINGH et al., 2019). It can damage their confidence and trust at a time.

d) Reputational loss: These cases can harm customer reputations as they can face false accusations on financial statements. In a phishing scenario, customers can face huge reputational damage through their banking statements.

e) Trust issues: Fraud activities can lead the customer to break trust in their financial systems via banks. In some cases, they think their customers are not doing enough to protect their information and security measures. Thus they stop utilising these online banking practices or seek other solutions. It can create a huge impact on banks as they can lose their potential customers and face reputational loss.

f) Consequences of legal works: Fraud cases can lead the bank towards legal consequences (Jibril et al., 2020). Banks also face punishments for failing to meet security standards for detecting fraud activities and monitoring all faults. If customers have disputes on their accounts, they can also face regulatory consequences through their banks.

Overall, fraud related to Internet banking can impact society, emotionally and financially on customers. Banks must serve quick protection against fraud to protect customers. With the help of vigorous safety techniques and monitoring records, banks can avoid the risk of future threats in the long term. Also, the banks must be prepared for upcoming risks as frauds are increasing rapidly in India.

2.6 Regulatory Framework for Banking Services in India

In India, the Reserve Bank of India (RBI) operates a regulatory framework, this institution is authorized for regulations, legal supervision, and monitoring of banking systems in this country. This framework of RBI increases efficiency, safety, and stability in the banking industry and keeps the customers constant with their services. There are several key factors in banking services can be seen in India, such as:

a) Banking Act of Regulation, 1949: This banking regulation act presents a proper framework to develop, form, and operate banks situated in India (Pazarbasioglu et al., 2020). It helps RBI empower with regulatory actions for example providing licences to banks, acquisition, and fixing accurate guidelines for banking operations.

b) Efficient regulations: RBI has implemented efficient regulations suitable for banks towards stable services. It involves small requirements of assets, classification of capital, reports against huge loans, preparation for future risks, and overall operational management.

c) Requirement for issuing license: Mainly the issue of licensing is handled by RBI. It shows clear criteria for the entry of a bank and it involves capital, future support, current plans, and strategic structure of formation (D'Silva et al., 2019). RBI also operates the entry of foreign banks in this country and they operate via planned guidelines and framework.

d) Customer safety: RBI implemented various robust measures to protect banking services for customers. It also developed guidelines for effective practices in solution mechanisms regarding risks. RBI also monitors non-banking monetary funds to assure customer trust through banks.

e) Deposit interest and credit guarantee corporation: It is a part of RBI for the stability of each type of customer. This plan ensures the deposit's safety whether the bank fails somehow.

f) Cybersecurity and technical advancements: RBI has set standards for the usage of technological features in banks that have clear practices of cyber security (Haralayya and Aithal, 2021). It changes according to the requirements of current times in online facilities.

g) Corporate politics: For banking services, RBI has fixed plans on corporate authorization. That involves the directors from sector boards, control systems, risk management, and necessary changes. All these regulations increase efficiency, transparency, and legal consideration in every aspect.

Overall, the framework implemented by RBI has been significant for providing better services in India. It plays a vital role in monitoring and operating whole services with new inventions, facilities, innovations, and promotions. This framework includes options for tackling issues and gaining confidence in recent banking systems.

2.7 Technological and Innovative Solution

Improving security is a top priority in Internet banking. Financial firms that recognize this can employ cutting-edge biometric authorization systems. Adopting machine learning (ML) and artificial intelligence (AI) appears to be a critical technique for reinforcing online banking systems (Yildirim and Varol, 2019). These tools can filter through massive databases,

evaluating user actions to spot abnormalities that might indicate a security compromise. Various intelligent interactions, operated by natural language processing (NLP), provide users with instant and customized support, efficiently responding to queries, granting transaction guidance, and even giving financial advice (Suryono et al., 2020). This additionally improves user interactions, but it also leads to a greater effectiveness and fulfilling user experience, decreasing dependency on traditional customer service channels.

Blockchain technology is starting to show itself as a revolutionary solution to data integrity and transparency problems. Blockchain creates an irreversible ledger by taking use of the fragmented and counterfeit-proof nature of transaction history. This lowers the dangers associated with errors and fraudulent activities while also boosting confidence in the reliability of financial transactions (Kitsios et al., 2021). With their more user-friendly interfaces, multilingual assistance, and educational resources, these apps empower users to manage their finances independently. Financial institutions give poor people access to banking services, which helps close the digital divide and advance a more just financial system.

Comprehensive resolution of online banking concerns necessitates the strategic incorporation of cutting-edge technologies. Financial organizations can create a strong, safe, and user-friendly digital banking environment by using biometric identification, AI, and blockchain technology (Niemand et al., 2021). This pre-emptive use of technological approaches not only tackles existing issues, but also places institutions at the leading edge of the growing digital environment, providing a robust, innovative, and accessible financial ecosystem.

2.8 Awareness and education level of customers regarding such fraudulent activities

Customers' knowledge and education expertise about various cyber dangers are critical in securing their finances in the ever-changing world of online banking. Despite the increasing complexity of cybercriminal operations, many consumers remain without a full understanding of risks such as phishing, theft detection, smishing, vishing, card skimming, virus and malware assaults, SIM deception, and other illegal online banking activities (Naeem and Ozuem., 2021). Clients' comprehension of Phishing, smishing (SMS phishing) and vishing (voice phishing) is mostly poor. Cybercriminals use such avenues to trick people into disclosing sensitive data or doing activities that jeopardize their security. Consumers are prone to social engineering efforts because they are unaware of these procedures.

Another key factor that requires consumer knowledge is the identification of theft. Numerous individuals are probably unfamiliar with the warning signals of a stolen identity or illegal access to their accounts (Ghelani et al., 2022). This information gap might lead to postponed responses to unusual behaviours, thus exacerbating the harm caused by hackers.

Card skimming, a practice in which fraudsters acquire card information using modified card readers, represents a hazard that demands more awareness. In order to prevent becoming prey to this type of fraud, consumers should be trained to know how to recognize and avoid corrupted ATMs or point-of-sale devices.

Malware and virus assaults represent serious threats to digital financial security. Although some clients may utilize antivirus software, it is critical to comprehend the shifting nature of cyber-attacks and take proactive actions to combat sophisticated assaults.

SIM fraud involves an emerging problem in which attackers attempt fraudulent techniques to get access to a consumer's cell phone number (Carbo-Valverde et al., 2020). A lot of consumers may be unaware of the hazards connected with SIM fraud including the need to properly safeguard their cell phones.

Despite technological developments, a significant part of clients remain uninformed about the many hazards of online banking. Giving clients the information they need to spot and counteract cyber dangers is critical to building a more robust digital banking environment.

2.9 Challenges in Internet Banking

Internet banking has revolutionized the way people handle their finances, providing unparalleled ease and availability. This technical development, however, cannot be considered without its drawbacks. From safety issues to consumer service challenges, financial companies must overcome various barriers to provide an effortless and safe user experience (Kaur et al., 2021). The ongoing threat of data breaches constitutes one of among the most significant issues in online banking. As money transfers shift online, cybercriminals and attackers develop more sophisticated strategies to exploit flaws in banking platforms. Phishing attacks, identity theft, and malware all represent substantial threats, necessitating large investments in sophisticated cybersecurity safeguards to protect sensitive consumer information. Keeping online transactions secure and personal information safe is a never-ending challenge that necessitates continual monitoring and innovation. Another issue is the heterogeneous technical

environment (Rahi et al., 2019). Internet banking may be accessed via a wide range of gadgets, including mobile phones, tablets, and PCs, each having its own set of safety features and weaknesses. It is a difficult effort to provide a uniform and safe experience throughout this heterogeneous environment. Banks must accommodate different platforms, browsers, and gadget specs while preserving a high degree of safety and functionality.

Customer knowledge is another barrier to overcome in the world of digital banking. Many consumers may be unaware of the hazards involved with online payments or the safety measures put in place by their institutions. It is a continuing struggle to educate consumers about recommendations for internet security, the significance of secure passwords, along how to identify possible dangers (Gayan Nayanajith and Damunupola., 2019). Financial organizations must engage in educational activities to educate people and decrease their vulnerability to cyber dangers.

Even while there are many advantages to online banking, there are also disadvantages. Financial institutions face a number of difficulties in maintaining the long-term sustainability and security of online banking, including cybersecurity issues, a diverse technological environment, issues with client confidence, and the need for ongoing education. The ways in which banks handle these challenges and give their customers a safe and reliable online banking experience have to keep up with technological advancements. Another major challenge with internet banking is maintaining regulatory compliance (Shankar and Jebarajakirthy, 2019). As the digital ecosystem evolves, so do the laws governing financial transactions and data security. Financial organisations with international operations have to navigate a complex legal framework, with various jurisdictions having their own set of regulations and laws.

Compliance with such requirements is additionally a legal requirement, yet it also proves critical for sustaining consumer and stakeholder confidence. Noncompliance can result in serious repercussions such as legal proceedings, financial fines, and reputational harm. Banks face continuing difficulty in keeping up with emerging regulatory structures and guaranteeing that online banking systems comply with these requirements.

2.10 Internet Banking Fraudulent Activities Cases in India

Internet banking fraud is often seen in India, especially during the time of the COVID-19 pandemic. There are several cases where the public has been seen being looted by cyber

criminals in India. Some of the cases are discussed below. On February 8th, 2023, a man faced fraud and abandoned almost 2.2 lakh rupees from his bank account. It has been reported that the man booked a cab from a reputed company but somehow it was not booked. After facing difficulties a man pretending to be an employee of that specific cab company introduced himself as Rajat and asked the man to pay 100 rupees on the website (India Today, 2023). But at that time as well the man faced another glitch while making the payment. He abandoned the process immediately. But later he discovered that transactions over 2lakh from his credit card were done without any authorisation. Despite blocking his credit card, the software engineer from Maharashtra lost 2.2 lakh rupees. The case is still being investigated by the cybercrime department of Maharashtra. This was a case of pharming, the hackers in this case manipulated the DNS of a legal website, and the website was redirected to another website that was created by the criminals. Despite typing the correct URL, the computer will redirect to the fraud website only and the hackers can easily enter into the person's every personal information.

In another case, a 70-year-old lady from Mira Road lost 8.3 lakh rupees while purchasing towels from an e-commerce platform. The towels which were of 1,170 rupees were charged 19,005 while making a purchase. The lady then called the bank for help with her transaction but no such help she got. After some time she received a call from an unknown number and the person over the phone pretended to be a bank employee. The person asked the lady to download an application for a refund. Instead, she lost another 1 lakh from her bank account without any authorization (INDIA TODAY, 2023). She rushed to the police station but in the meantime, the fraudsters took 8.3lakh rupees from her bank account. In this case, the fraudsters however convinced the lady to download the application and then they got access to every personal detail like bank account number, OTP, and others.

2.11 Literature gap

In the framework of an in-depth examination of the socioeconomic and technological factors that impact the acceptance and efficacy of digital banking services, the study's literature deficit on digital banking and its issues is significant. While the existing literature comprehensively covers the benefits and conveniences of online banking, there is a scarcity of studies that dive into the multifaceted issues encountered by both banks and individuals. Given the rising frequency and complexity of online assaults, there is an imperative to research the emerging cybersecurity risks in the field of online banking. Furthermore, previous research frequently ignores the influence of socioeconomic variables such as computer proficiency, cultural

attitudes, and confidence on the uptake and long-term usage of online banking services. Knowing these characteristics is critical for developing successful methods for closing the digital gap and ensuring the accessibility of online banking services.

2.12 Summary

The content stipulated discusses the essential elements of digital banking safety, the impact on consumers, the regulatory environment in India, fraudulent cases in India, customer awareness, internet financial services challenges, technological solutions, and real-life cases of digital banking fraud in India. This review focuses on the significance of safety metrics, the many sorts of fraudulent activity, and the resultant impact on consumers' finances, mental well-being, and faith in the financial sector. It also dives into the Reserve Bank of India's (RBI) rules and regulations and the obstacles that online banking faces, such as cybersecurity concerns and legal compliance problems. The material presents novel technology methods to improve Internet banking security, including biometric authorization, artificial intelligence, and blockchain. Furthermore, client awareness and education about fraudulent activity is emphasized as critical aspect of risk mitigation. Real-world examples highlight the system's flaws and underline the importance of ongoing monitoring and education. The literature gap part emphasises the importance of conducting a more in-depth study regarding the socio-economic and technical factors impacting the acceptability and success of online banking services. In general, the in-depth debate sheds light on the intricacies and limitations of digital banking in India.

Chapter 3: Research Methodology

3.1 Introduction

The previous chapter of this study describes various literature with respect to the current research study. Based on the previous chapter, a significant amount of information was provided that helps in describing and understanding the research topic in an effective way. In this current chapter, the selected research methodologies are described and justified. Research methodology is one of the most crucial aspects of this study. It is one of the most crucial chapters of this study as it provides efficient information on the way this research is conducted. This chapter describes all the selected methodologies implemented in this study. Research methodology is referred to as a systematic process that is taken into consideration such that the research study is carried out in an effective way and the research aims as well as objectives are accomplished (Newman and Gough, 2020). This chapter includes various aspects such as research philosophy, approach, method, design, data collection method, and analysis, which is further justified by the researcher for selecting those particular aspects of this study. In addition to this, this chapter also includes information on the limitations faced by the researcher while carrying out this study. Apart from these, the ethical considerations taken into consideration by the researcher are also highlighted in this chapter.

3.2 Research philosophy

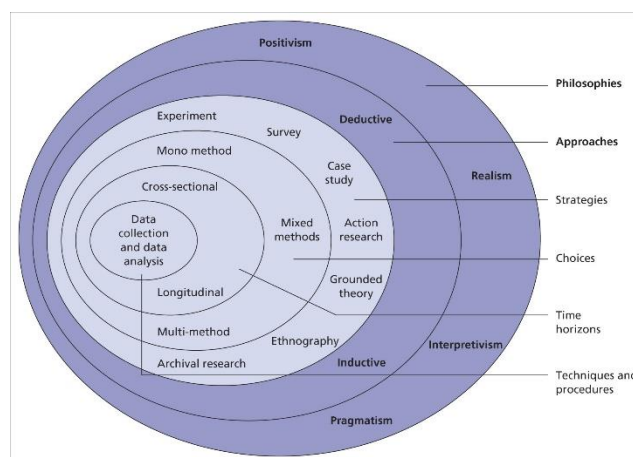


Figure 3.1 Research Onion

(Sources: Newman and Gough, 2020)

Research philosophy is referred to as a belief regarding the way data about any phenomenon is required to be collected, analyzed as well as utilized (Newman and Gough, 2020). In addition to this, it is also found that the research philosophy is related to assumptions, knowledge as well as characteristics of the study. Research philosophy is also associated with certain ways that include the development of knowledge. It is further opined by Al-Ababneh, (2020) that research philosophy mainly deals with the nature, source as well and development of knowledge. On an overall basis, it is found that research philosophy deals with formulating assumptions as well as beliefs.

There are two major types of research philosophies, which are positivist research philosophy and the other one is interpretivist research philosophy. However, the selection of an appropriate research philosophy is mainly impacted by several practical implications. Research philosophy is crucial for a research study as it helps in laying the foundation of the study. (Al-Ababneh, 2020) added that research philosophy has a direct impact on the research methodology, which involves research design, data collection as well as analysis methods. Therefore, it is crucial to have a better understanding of the philosophy that inspires the study to ensure that the rest of the decisions for carrying out the research method are aligned.

3.2.1 Positivism philosophy

Positivism philosophy is referred to as the philosophy that focuses only on factual knowledge that is mainly collected through observation, which also includes measurement, and is one of the most trustworthy philosophies. According to Budianto (2020), the researcher who implements the positivism philosophy has a limited role in collecting data and interpreting the collected data in an objective way. Positivism philosophy is mainly dependent upon the quantifiable observations that eventually require statistical analyses, and is regarded as one of the most dominant research types when business as well as management fields are concerned. It is further noted by Greening (2019), that positivist philosophy is mainly carried out in accordance with the empirical view that knowledge can be gained and developed from human experiences. Positivist philosophy provides an ontological view of the world in the form of observable elements as well as events interacting in a determined and regular way.

3.2.2 Interpretivism philosophy

Interpretivism is another form of research philosophy, which includes the interpretation of elements present in a study. In this regard, Budianto (2020) states that in interpretivism

philosophy, researchers mainly assume that reality can only be accessed through social relationships, such as consciousness, language, shared meanings as well as instruments. Dodds and Hess (2020) argued that interpretivism philosophy development is mainly done on the basis of the critique collected from a positivist view with respect to the social science aspects. In this regard, it can be said that interpretivism philosophy mainly focuses on qualitative analysis. Further, it is added by Greening (2019) that interpretivism takes a philosophical approach into consideration mainly emphasising the importance of interpreting societal norms in order to be understood easily. On the basis of the above part of this section, it is identified that interpretivism is inversely proportional to positivist philosophy.

3.2.3 Justification for choice of philosophy

On the basis of this present study, the researcher has taken *positivism* philosophy into consideration. The researcher has selected the positivist philosophy for this study because according to Mahuika and Mahuika (2020), the researcher believes that human and societal behaviour is objective and one can easily measure it by implementing scientific and quantitative methods. Hence, in order to understand the role of Internet banking in identity theft and fraudulent activities, the researcher needs to implement a positivist philosophy. As stated above, this philosophy considers a quantitative approach, and considering quantitative data for this study would help in objectifying the overall findings of the study in an effective way. This present research has offered verifiable proof to back up its outcomes by gathering as well as evaluating information on real-world incidents of online banking crime in this nation. Furthermore, this philosophy has offered trustworthy confirmation which assisted this dissertation's outcomes with the help of the collection of real-life data and analysis of those data in a critical manner. Additionally, this philosophy has proved beneficial in evaluating the efficacy of financial procedures, laws, and safeguards in various areas of this nation. The researcher was able to collect a lot of data on Internet banking and banking-related frauds and thefts with the help of this philosophy which has given this dissertation more consistency in the findings and conclusion.

3.3 Research approach

The term “research approach” has different meanings associated with it. Some of the researchers state that the research approach describes the method implemented for collecting and analyzing data for the study; whereas, some researchers state research approach is a difference present between quantitative and qualitative methods (Dzwigol, 2022). However,

Mahuika and Mahuika (2020) described the research approach as a general procedure considered for carrying out a research study. In this regard, the research approach is mainly segregated into two types, (a) Inductive approach and (b) Deductive approach. The significance of the hypotheses prepared for the study is the main point of distinction between these two approaches. According to Dzwigol (2022), the deductive approach is mainly used for testing the legitimacy of hypotheses, and the inductive approach is mainly used for generalizing or developing theories.

3.3.1 Inductive approach

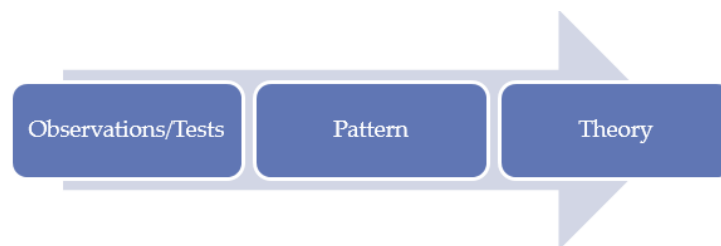


Figure 3.2: Inductive approach process

(Sources: Ocaña-Fernández and Fuster-Guillén, 2021)

When an inductive approach is taken into consideration, it is found that in this approach there is no need to formulate the hypotheses. In this approach, the researcher starts the study with the research questions, along with the aim as well as objectives of the study that are required to be accomplished during the research study (Dzwigol, 2022). In an inductive approach, the research study primarily emphasizes answering the research questions and implying new theories for the study that resonate with the problem statement of the study. Ocaña-Fernández and Fuster-Guillén (2021) opined that the inductive approach is a method where the researcher is found to accumulate and analyze data for developing theories, hypotheses, or concepts on the basis of the patterns as well as observations observed from the accumulated data. The inductive approach implements a bottom-up method where the researcher starts with certain observations and then moves upwards towards more generalized ideas as well as theories. Babii (2020) further added that an inductive approach is mainly used in exploratory studies or in those studies, where the major part of the research topic has not been researched or studied before.

3.3.2 Deductive approach

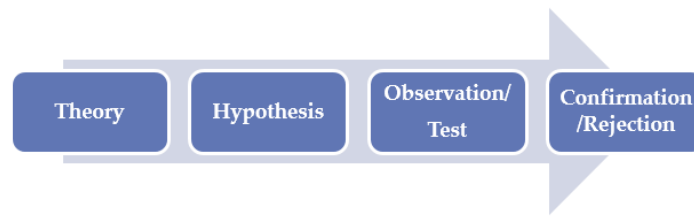


Figure 3.3: Deductive approach process

(Sources: Babii, 2020)

In a study, if the researcher has articulated a certain set of hypotheses, which is further required to be accepted or rejected while carrying out a research process, then it is required to implement a deductive approach (Ocaña-Fernández and Fuster-Guillén, 2021). With the help of this approach, the role of Internet banking with respect to fraudulent activities as well as identity theft is evaluated by formulating hypotheses that are required to be tested during the research study. With respect to the deductive approach, the researcher initially starts by developing a theory, hypothesis, and generalization and further examines those developed hypotheses by collecting data or observations (Ryder et al. 2020). Generally, in a deductive approach, a top-down method is taken into consideration, where the researcher initiates the study with a common idea and further tests that idea through appropriate observations. This type of research is also used for confirming a theory or the stated hypothesis.

3.3.3 Justification for choice of approach

In the context of this present study, the researcher has selected a **deductive** approach. In this present study, the researcher has selected this approach because in this study the researcher aims at exploring the relationship between Internet banking and the cases of fraudulent activities and identity theft. This approach is helpful for this study because the study is required to test certain hypotheses that are formulated from current theories and established concepts for a particular study (Babii, 2020). In this present study, the researcher initially starts with pre-stated theories for analysing the role of Internet banking in fraudulent activities and identity theft by accumulating required data and further assessing it. Since this approach is based on numerical information, it is simpler to evaluate as well as analyse the frequency of stolen identities as well as digital fraudulent transactions. Due to the result of the numerical information gathering methods used in this dissertation, noteworthy results have been obtained that improve our knowledge of the scope as well as trends of crime in populous nations

including India. Hence, due to these reasons, the researcher has selected a deductive approach over an inductive approach.

3.4 Research design

Research design is an important as well as systematic framework that mainly defines the overall structure as well as the plan for carrying out a research study (Ryder et al. 2020). It acts as an outline that guides the researchers on the way to collect, analyze, and interpret data for addressing the research questions. It is important to ensure that the researcher selects the appropriate research design because an appropriate research design helps to ensure the validity, reliability as well as the overall success of the study. The research design also includes decision-making regarding several aspects of the research process, methods for data collecting, sampling strategy, and analyzing data. (HR and Aithal, 2022) added that research design is impacted due to the type of research questions, theoretical framework, and limitations of the study. Apart from this, HR and Aithal (2022) stated that generally there are three types of research designs, which are *explanatory design*, *descriptive design*, and *exploratory design*. On an overall basis, it can be said that research design is an inclusive procedure used for guiding the researchers such that they carry out a systematic study. It deals with various aspects of the research. The eventual aim of the research design is to ensure that valid and consistent results are found that have a significant contribution to the specific field of study.

3.4.1 Explanatory design

Explanatory research design is defined as exploring all the areas to determine why certain outcomes occur. In other words, HR and Aithal (2022) stated that explanatory research design is a type of research method that analyses all the possible actions to figure out the reason behind something happening. This is the best type of research design suitable when limited to no information available for the researcher to conduct research. This type of research design helps to increase the knowledge and information of the researcher on the research topic. It includes a detailed understanding of the cause or the phenomenon (Reddy, 2020). Due to these aspects, it becomes easy for the researcher to predict the future occurrence of the same issues and recommend certain ideas that will help in developing the situations into positive ones. The researcher selects this research design where less information is present and needs more attention in future.

3.4.2 Descriptive design

Descriptive research design is an exceptional and powerful tool used by the researcher while conducting a study to gather or collect information about a particular subject or cause (Firdaus et al. 2021). This type of research design tool is used by the researcher to analyse the information collected about the phenomenon which will provide detailed information or a picture. A detailed picture provides accurate information and characteristics of the particular subject or cause under study. As opined by, Reddy (2020) have stated that descriptive research design collects and analyzes every detailed information effectively such that accurate predictions or hypotheses can be defined. In other words, the researcher analyzes the subject based on when, how, what, which and where in a particular situation or subject which helps in identifying underlying reasons and opinions that help in conducting research for a better explanation of the issues and future ideas for betterment (Firdaus et al. 2021).

3.4.3 Exploratory design

Exploratory research design is a type of research methodology that studies or investigates effectively all the issues and problems that have not been studied in the past. Patel and Patel (2019), have stated that exploratory research design helps the researcher in collecting and analysing data and information about the research topic that was not studied in past. This design is effective enough to define an accurate picture and analyse all the areas which are positive and negative. This research design gives complete freedom to the researcher to define the problem areas and recommended areas for further studies. The researcher mainly uses primary data for further analysis to drive the nature and characteristics of the subject. However, in many cases, it is also seen that a large sample of data is collected in an explanatory manner such as those represented through quantitative data analysis.

3.4.4 Justification for choice of research design

From the above description of three research designs, a favourable choice of research design is the Exploratory research design. The reason the researcher selected an exploratory research design to conduct this study as it helps them collect a large sample of primary data and represent them through quantitative data representation. The researcher was able to define certain issues and also reasons behind those issues which leads to explaining the problem and analysing certain grounds to mitigate them. In this study, the researcher collected data from the 60 respondents through survey methods from the customers of banks. This has rendered it easier for the researcher to assess the measures taken by financial institutions and consumers to guard against fraudulent activity on the internet. Moreover, the researcher was permitted to conduct

this investigation broadly by thoroughly examining the issue formulation by putting this method into practice. As financial constraints could have become a key area of concern, therefore, this design was selected as it has a reputation for low cost and gathering of data on internet banking in fraud and identity theft in India quickly.

3.5 Research Strategy

It is defined as a process that defines a broad plan of action that shapes the researcher's thought process. As opined by, Patel and Patel (2019) have mentioned that research strategy helps the researcher in conducting the research systematically and effectively as per the scheduled deadline. There are different types of research strategies, but in this study, a researcher has selected a primary research strategy while conducting this study. In this study, the researcher obtained first-hand raw data and information that was analysed and gathered to derive the solutions to the problem statement of this study. The first-hand information gathering made possible by this strategy reflects the present situation of electronic financial scams in this country. Moreover, this is especially crucial in an area that is changing swiftly, including safety concerns, where unexpected concerns as well as deficiencies might appear at any time.

3.6 Data collection tools and methods

Data collection is defined as the process of collecting data and information from different sources which provides accurate and effective information. Hughes and Barlo (2021), have stated that data collection is a methodical and predetermined way chosen by the researcher for analysing and collecting data as per the study needs. While carrying out the study, the researcher uses the data and information to answer and elaborately illustrate all the research questions and hypotheses to derive a useful outcome for better future application. Data collection is generally of two types qualitative and quantitative data collection respectively.

In this study, the researcher has selected a quantitative data collection method. Quantitative data collection is a process of collecting numerical data and information which are analysed by implementing statistical methods. Moreover, quantitative data collection has been crucial for this study since it was linked with human responses which has assisted this study to increase its standard by deploying real-life evidence. In other words, it can be said that in this study, the researcher has used primary data by implementing a quantitative data collection method. In this study, researchers have implemented a survey questionnaire method to the 60 respondents who are the customers of the bank. This data was further analysed and represented to derive the solutions for the problem statement of this study.

3.7 Data analysis

Data analysis is the process that involves inspecting, analysing, and transforming the collected data and information. As opined by Hughes and Barlo (2021), have mentioned that data analysis is the process of systematically application and choosing effective data analysis techniques that involve statistical methods or logical methods to illustrate and describe the data and information collected for data evolution. In this research, among two data collection methods, the researcher has selected a quantitative data analysis method. In other words, the quantitative data collection method has helped the researcher implement effective data by collecting primary data for a better analysis of the problem statement. In this research, the gathered evidence has been represented graphically by the scholar, who has carried out the assessment in a statistical manner. Furthermore, the replies of those who participated in the questionnaire inquiries have been displayed and critically discussed via the use of graphics of the pieces of evidence, which has also guaranteed the extraction of useful details for the purpose of producing helpful findings from this research. Furthermore, the method of assessment has provided this dissertation with a helpful collection of explanations for comprehending the implications of online banking's participation in fraud and identity theft in India.

3.8 Ethical Consideration

Certain criteria must always be followed when conducting a research study, and it is the researcher's responsibility to follow those regulations. Several considerations are made when gathering data for trustworthy sources. The ethical concern needs to be sufficiently compelling to ensure that the investigation proceeds. When obtaining details and information from customers, investigators have ensured that all standards and laws are followed. Participants in the interviews that were conducted were neither paid nor subjected to coercion to compensate for their data or opinions. Furthermore, by protecting the privacy of each respondent's name, phone number, and residency, researchers have improved the data's usefulness for a legitimate purpose. It is crucial to uphold ethical principles when carrying out a research study since it directs the investigator to reject and discard any material and information that has been obtained unethically or that has been manipulated. The data and information gathered for the study project will only be used for this purpose; it will not be used for any kind of commercial objective, and it will not be misused in any way.

3.9 Research limitation

This study is based on primary data which is collected from the customers of the bank. All the outcomes of this study highlight that respondents have implemented in the past or present issues they are facing while dealing with online banking. This study is only limited to a certain extent that explains the customer's point of view. In the future researchers might carry out this same study by analysing the strategy taken by the banks to prevent online fraud and also illustrate the viewpoint of the cyber-security employees to prevent this issue.

3.10 Research Timeline

3.11 Summary

This chapter, named Research Methodology, explains all the research strategies, design, data collection and analysis that were selected by the researcher while conducting this research. Few justifications and broad discussions are presented such that the reason for opting for a specific type is justified. Every research project requires to be executed correctly, however in addition it needs to follow ethical guidelines that protect the confidentiality of respondents and ensure producing high-quality scientific publications. This chapter provides a detailed explanation of the aspects of the investigation's methodology that will be considered in the appropriate development, analysis, and interpretation of the data and conclusions.

Chapter 4. Data Analysis and Findings

4.1 Introduction

In the above chapters, the researcher has mentioned all the aspects that were implemented to carry out this research from the data collection to the research approach, data analysis and research design. But in this chapter, all the data that has been collected from the 60 respondents through the survey questionnaire method is represented and analysed to derive the solutions to the problem statement of this study. Here researchers have explained and analysed the information that respondents have provided regarding the theft or issues they are facing regarding online bank transactions. At the end of this chapter, a clear and detailed explanation of the information will be presented on the basis of which recommendations and the future scope of the study will be discussed in the next chapter.

4.2 Quantitative Data Analysis

Question 1. How frequently have you encountered fraudulent activities in your Internet banking transactions?

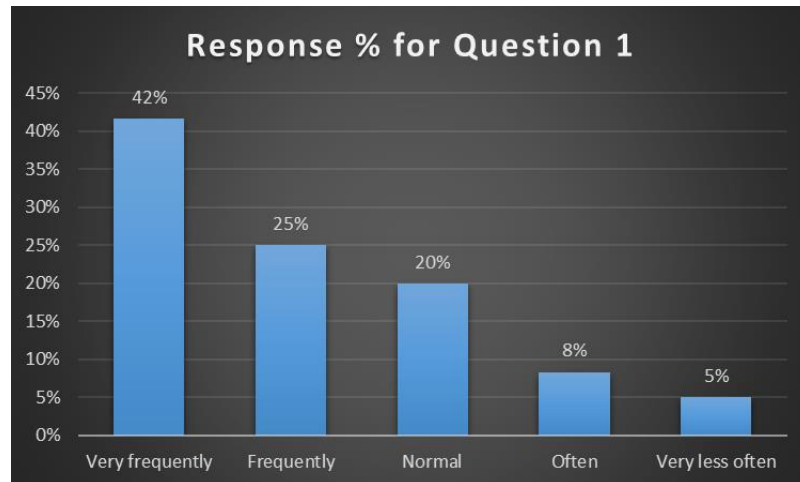


Figure 4.1 Respondents response for question 1

(Source: Created by researcher)

It can be understood that the majority of the respondents have faced fraudulent activities while they have opted for Internet banking transactions. This data has illustrated that most of the customers in this developing nation have faced issues with Internet banking services. From the responses, it is quite clear that the instances of fraudulent activities are quite high in India and the banking sector needs to keep a close eye on this to overcome the problem by increasing customer safety processes.

Question 2. How far do you agree that current online banking infrastructure effectively addresses the level of fraudulent activities?

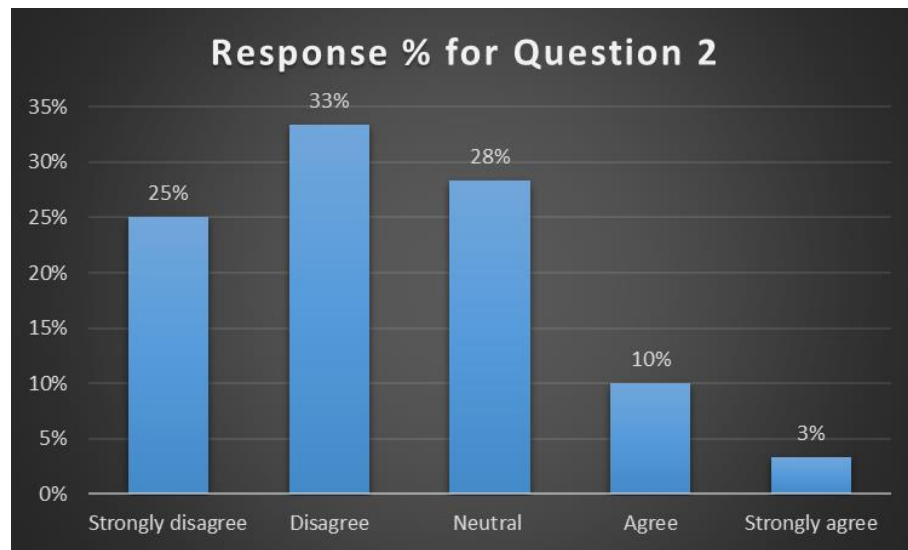


Figure 4.2 Respondents response for question 2

(Source: Created by researcher)

As per the respondent's responses, it can be understood that the majority of the respondents who are opting for online Internet banking for their transactions are not pleased or favour the banking infrastructure implemented to address the level of fraudulent activities. It is evident that there are not so many activities that can help the customers to ensure that they do not face fraudulent activities since fraudulent activities are not advanced in India. However, the selection of the neutral option by 28% of respondents also indicates that people have less knowledge on this which is not good.

Question 3. Have you ever personally experienced vulnerabilities in the security of your online banking platform?

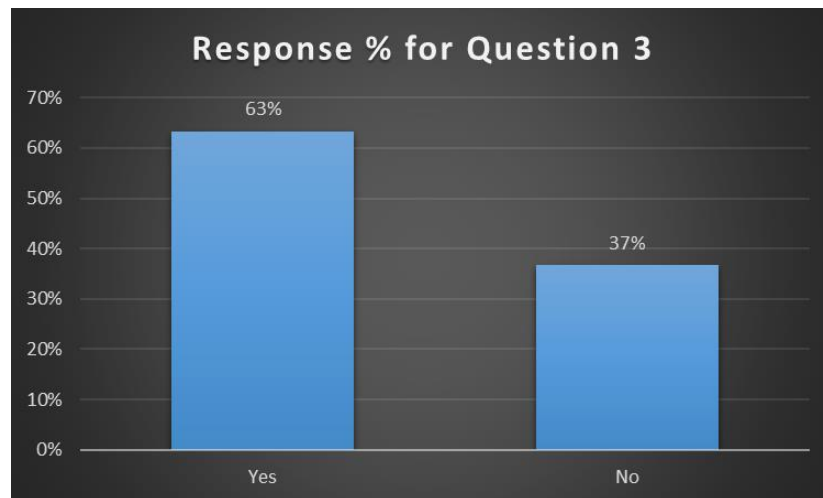


Figure 4.3 Respondents response for question 3

(Source: Created by researcher)

From this representation, it can be stated that the majority of the respondents have faced issues and are not comfortable with the security provided by the online banking platform. Personal experience is not good at all and the banking sector must find some strategies to overcome these obstacles. Since customers are the end-users of online banking platforms, therefore, to ensure that customers do not face issues, tactical interventions are highly required in the Indian internet banking domain.

Question 4. How far do you think cyber-attackers have become more sophisticated in their strategies over the past few years?

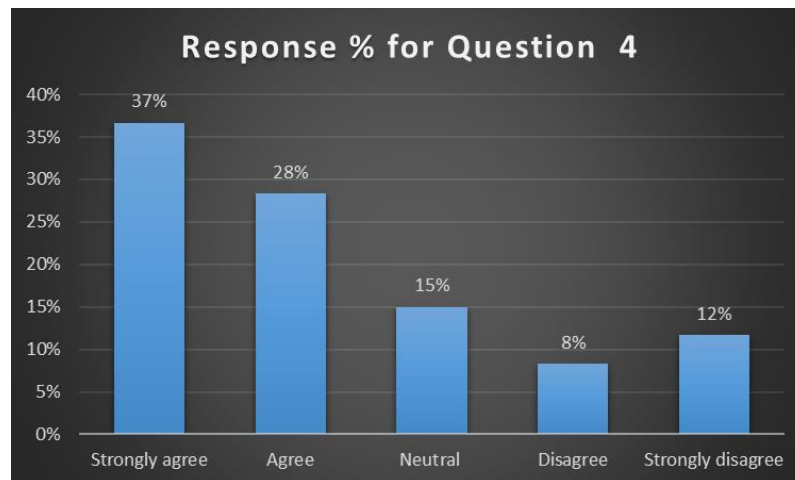


Figure 4.4 Respondents response for question 4

(Source: Created by researcher)

From this interpretation, it can be understood that respondents believe that cyber-attackers are utilising new technology and software to breach the security used by online banking platforms. From the respondent's responses, it can be concluded that respondents are aware that cyber-attackers are keeping up with the technology for fraudulent activities. Furthermore, the responses indicate that the assaults are growing in sophistication, targeting, reach, and frequency while going unnoticed for the most part. The bulk of these assaults have monetary motives. It is also true that there exists a rise in determined, malware, alongside spam assaults on online banking services.

Question 5. To what extent do you believe cyber-threats can impact the psychological well-being of individuals using online banking?

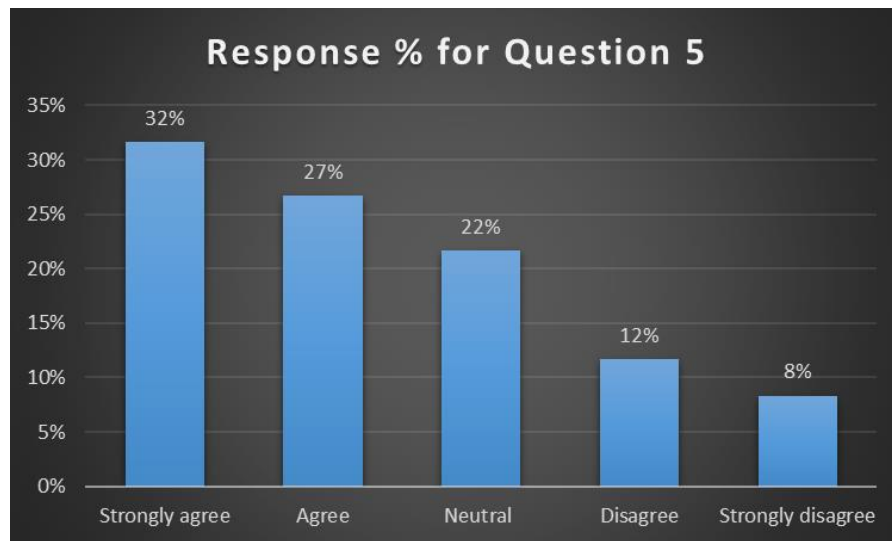


Figure 4.5 Respondents response for question 5

(Source: Created by researcher)

From this response of the respondents, it can be understood that the majority of the respondents believe that cyber threats are impacting the psychological well-being of those users who are opting for online banking services. Moreover, from the responses, it can also be concluded that Cyber-attacks have the potential to cause serious mental anguish in addition to monetary losses. Additionally, a reduction of faith in digital systems in online banking platforms in India can increase worry, as well as a sense of powerlessness can result from breaches of confidentiality.

Question 6. How far do you agree that there are specific risks associated with mobile banking compared to traditional online banking?

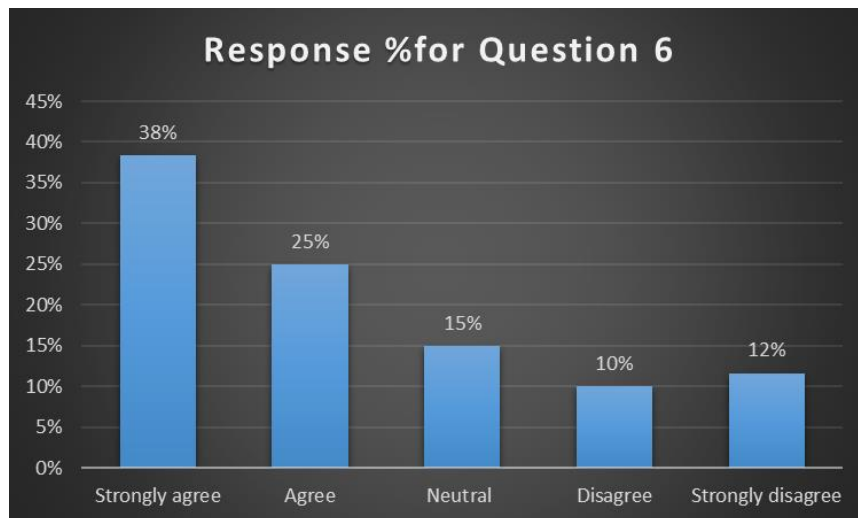


Figure 4.6 Respondents response for question 6

(Source: Created by researcher)

From these responses, it can be concluded that the majority of the respondents completely agree that mobile banking involves much more risk as compared with traditional online banking. Furthermore, among the main concerns raised by these respondents appears to be the lack of in-person customer assistance offered by mobile banking. Customers are limited to registering and lodging grievances online through chatbots, messages, or support lines. In a developing nation like India, this is a matter of concern since financial issues get a higher priority among Indians.

Question 7. How would you rate your awareness of cybersecurity practices related to online banking?

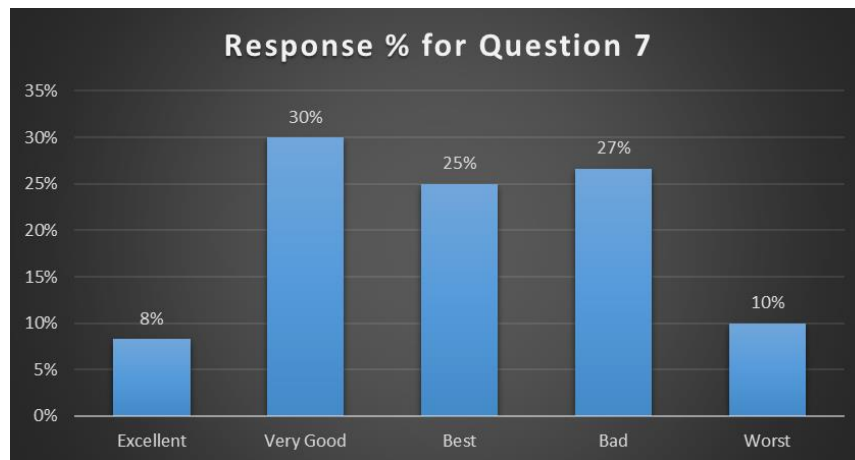


Figure 4.7 Respondents response for question 7

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of the respondents are aware of the cyber security practices related to online banking. However, it is still a matter of conflict since respondents have gone for positive and negative responses which indicates that they have distinctive knowledge about this matter. Indians must have more accurate insights and knowledge about cybersecurity practices related to online banking since it is all about them and this is how they can take significant steps to secure their monetary assets.

Question 8. How frequently do you update your passwords and security settings for your Internet banking accounts?

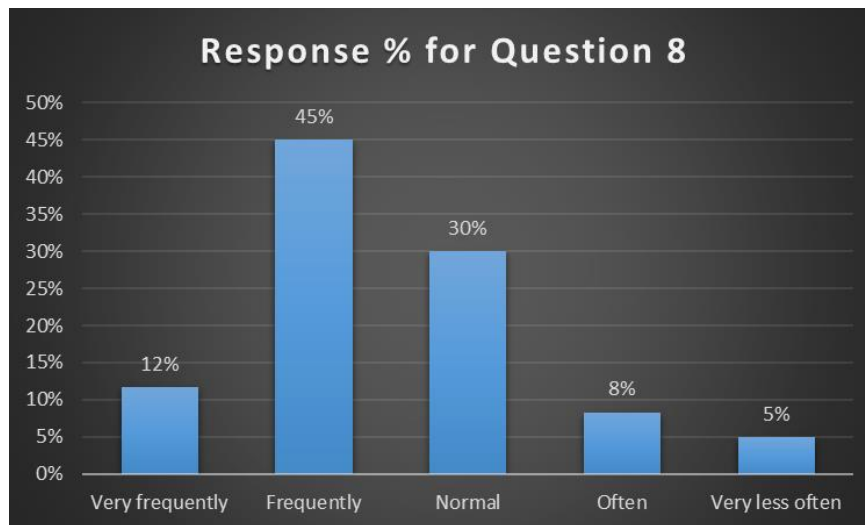


Figure 4.8 Respondents response for question 8

(Source: Created by researcher)

From this interpretation, it can be understood that the majority of the respondents update their passwords and security for their Internet banking accounts to prevent cyber security issues. Moreover, it is a good sign that they change their passwords frequently which assists them to secure their Internet banking accounts from getting scammed. However, the concern is still there since 30% of the respondents do not frequently change or modify their passwords and security settings which may cause them huge financial damage.

Question 9. How far do you think there is sufficient awareness about cybersecurity among users in densely populated areas?

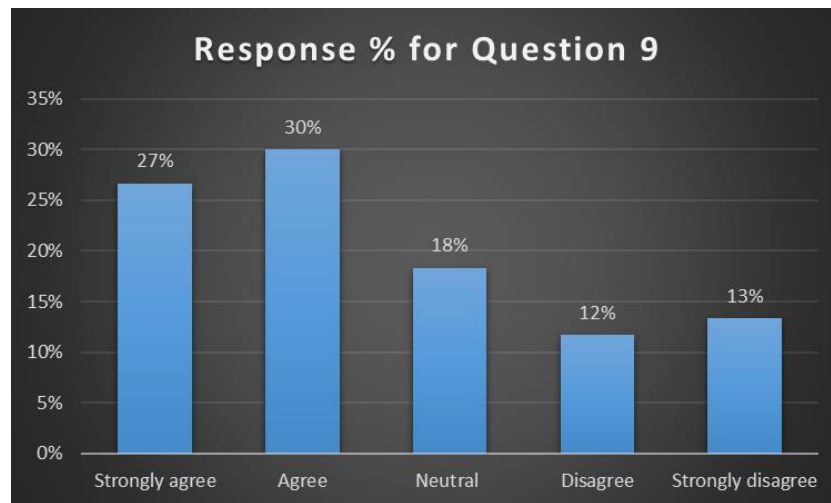


Figure 4.9 Respondents response for question 9

(Source: Created by researcher)

From this interpretation, it can be understood that sufficient awareness regarding cyber security among users is spread in densely populated areas. It should be noted that protection consciousness instruction in these domains assists users in mitigating the danger of harmful actions of cybersecurity. Moreover, it is obvious that the online banking sector can guarantee that user details are secured and shielded from cyber-attacks by giving customers in those regions the information and abilities they require to remain shielded electronically.

Question 10. Would you be open to using additional security measures, such as two-factor authentication, for online banking?

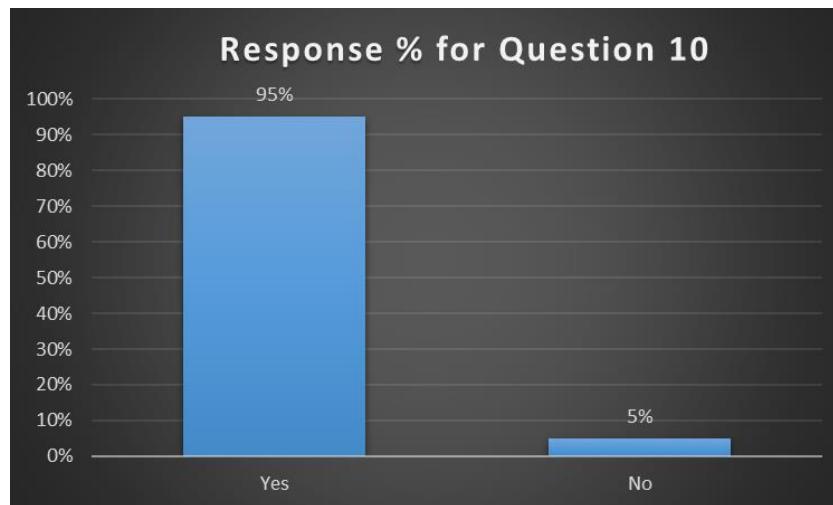


Figure 4.10 Respondents response for question 10

(Source: Created by researcher)

From this interpretation, it can be concluded that respondents are open and agree to use two-factor authentication or any other additional security measures while using online banking for their transactions to prevent fraudulent activities. It is undeniable that scams directly affect online banking platforms as data breach instances rise. In addition, despite the fact they had nothing to do with the theft, individuals who become subject to theft in India prefer to steer clear of online banking platforms. In this regard, two-factor authentication provides an additional security level that maintains websites safe.

Question 11. How confident are you in recognizing and avoiding potential cyber threats in online banking?

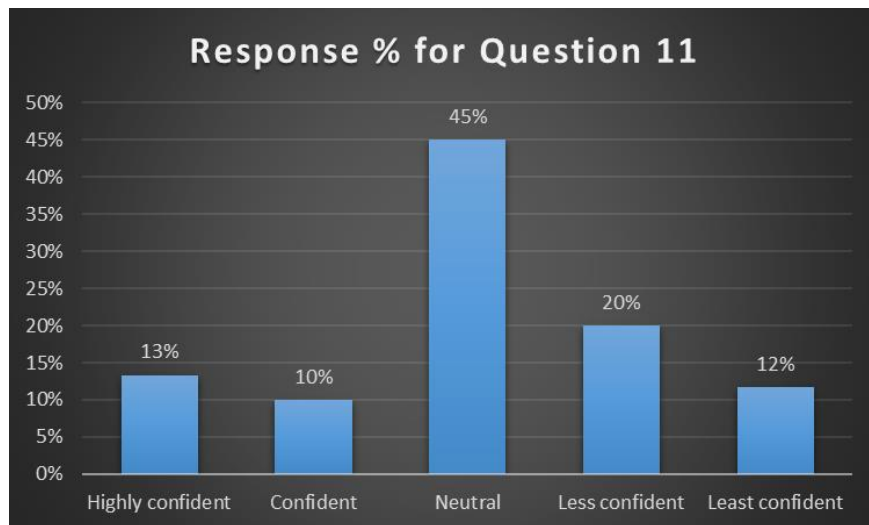


Figure 4.11 Respondents response for question 11

(Source: Created by researcher)

From this interpretation, it can be said that the majority of the respondents are neutral which means that are not sure about recognizing and avoiding potential cyber threats in online banking. Moreover, the lack of knowledge about recognizing and avoiding potential cyber threats in online banking has been causing huge damage to those users who use various internet-based platforms. Financial loss is the major factor here and the Indians need to get more insights about this to ensure that their online banking account stays safe and secure during and after transactions.

Question 12. Have you ever received phishing emails or messages related to your online banking account?

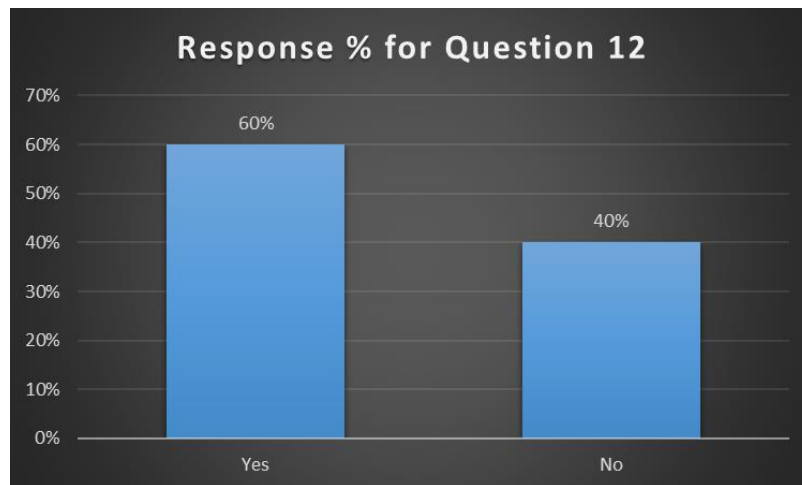


Figure 4.12 Respondents response for question 12

(Source: Created by researcher)

From this interpretation, it can be said that the majority of the respondents have received phishing emails or messages related to online banking accounts. The “No” response indicates that there is a massive blunder in the process and system inside the online banking system in India. Without getting phishing emails or messages related to their online banking account, users are unable to know about the issues which can also foster the concern of trust and loyalty. It can also trigger psychological problems.

Question 13. How often do you think financial institutions should provide updates or notifications regarding cybersecurity measures?

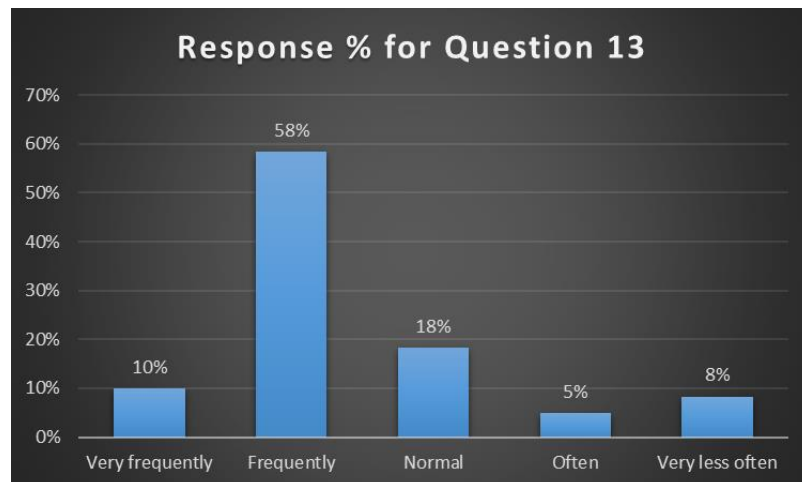


Figure 4.13 Respondents response for question 13

(Source: Created by researcher)

From this interpretation, it can be stated that the majority of the respondents have responded as frequently and very frequently. In other words, they agree that financial institutions need to provide updates and notifications regarding cybersecurity measures to their online banking users. It is indeed compulsory for financial institutions to provide updates or notifications regarding cybersecurity measures and that is how the account of the users can stay safe and secure. There are certain laws and policies about this matter and it is the responsibility of financial institutions to maintain those regulations and users in India must have knowledge on that as well.

Question 14. How far do you believe there is a need for increased education and awareness about online banking security?

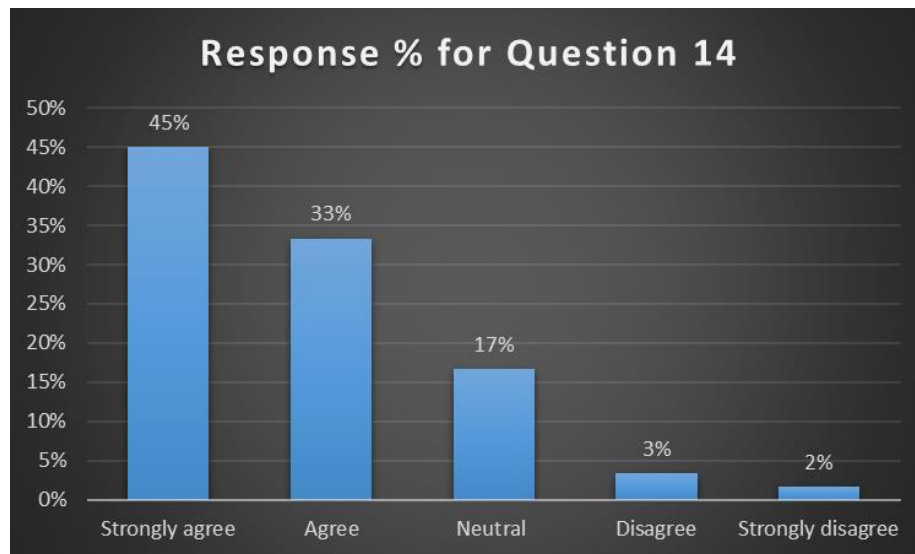


Figure 4.14 Respondents response for question 14

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of the respondents believe that there is a need for increased education and awareness about online banking security which will educate and raise the awareness of the cyber security of online banking users to prevent fraudulent activities. In addition to helping online financial institutions retain consumers' faith as well as respect in the online financial sector, cybersecurity serves as crucial for keeping their funds confidential and protected. Moreover, the most recent safety precautions must be used by online banking institutions in a developing country like India to safeguard the monetary activities as well as private data of their clients.

Question 15. how would you rate the impact of cyber threats on your behavioural aspects related to online banking?

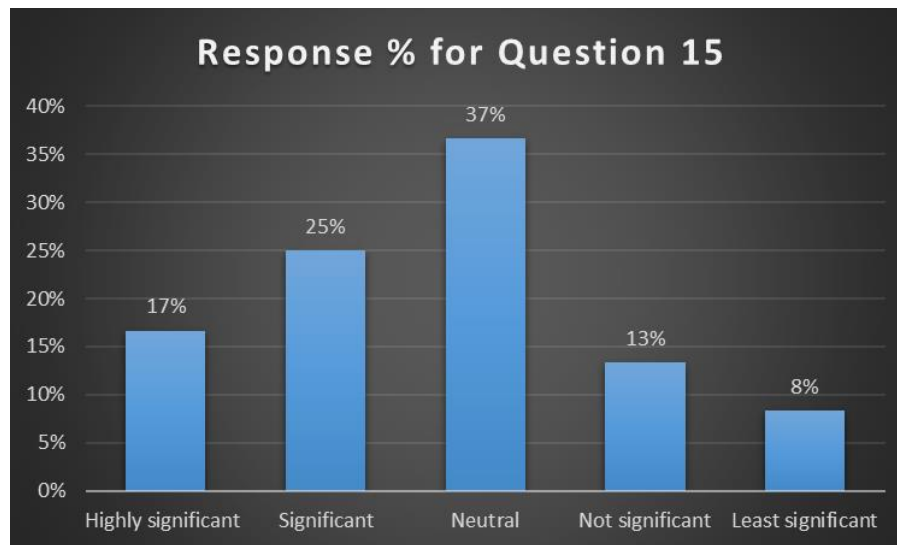


Figure 4.15 Respondents response for question 15

(Source: Created by researcher)

From this interpretation, it can be concluded that cyber threats are impactful on the behavioural aspects of the respondents related to online banking fraudulent activities. In other words, it can be derived from the respondent's response that the impact of the cyber threats is affecting the behavioural aspects of the customers of online banking services. Moreover, in this regard, a few studies on a broader scale with the involvement of more respondents are required to judge this matter more accurately and effectively.

Question 16. How far are you satisfied with the strategies implemented by your online banking provider to prevent cyber-attacks?

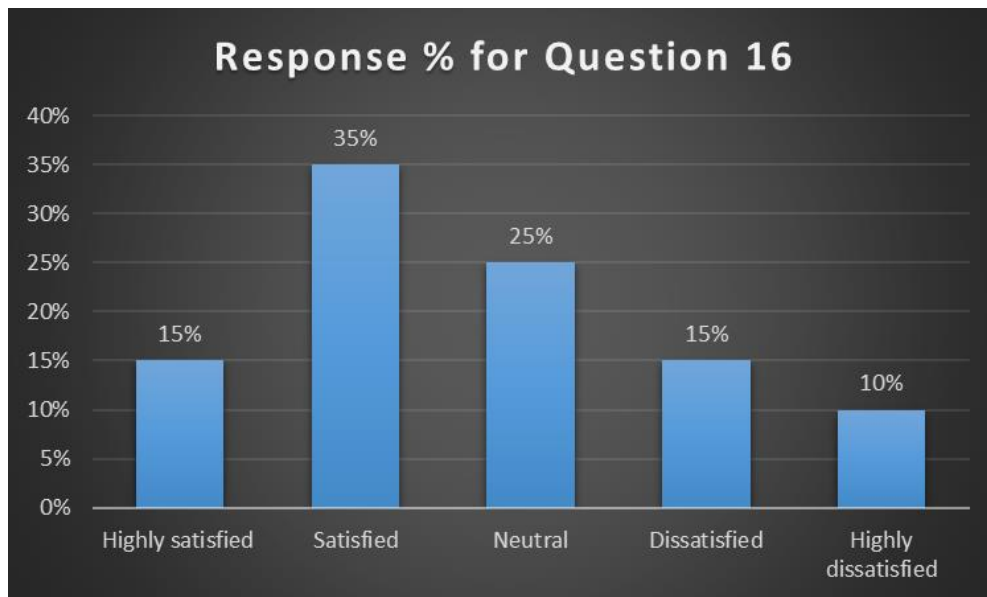


Figure 4.16 Respondents response for question 16

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of the respondents are satisfied with the strategies implemented by the online banking provider to prevent cyber attacks on online banking platforms. In other words, customers or users are satisfied with the strategies implemented by the online banking provider as it helps the users in preventing online fraudulent activities. It can be added that in the changing perspective of online processes, new strategies must be discovered and applied to ensure that the accounts of users are safe and online transactions are done securely.

Question 17. Have you attended any cybersecurity awareness programs or workshops provided by your bank?

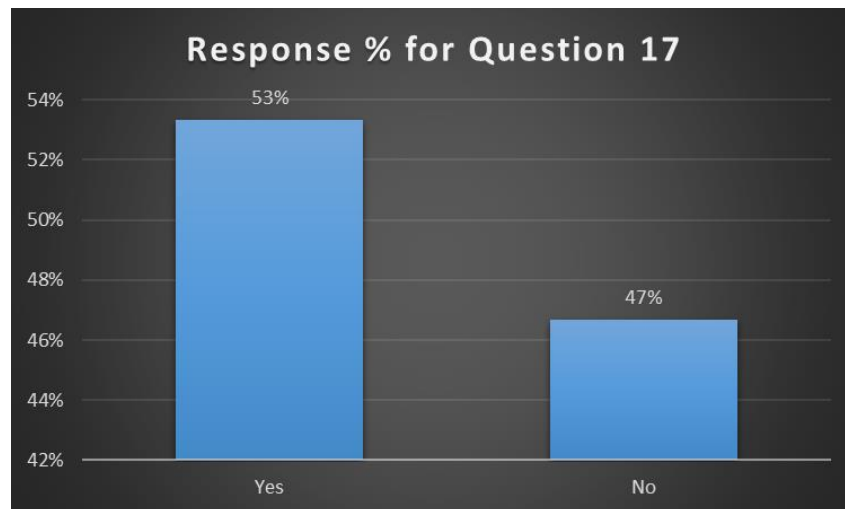


Figure 4.17 Respondents response for question 17

(Source: Created by researcher)

This interpretation concludes that few banking services and financial institutions are providing cybersecurity programs and workshops as a measure of increasing awareness and educating their users or customers. However, many respondents have mentioned that they did not attend any cybersecurity awareness programs or workshops provided by their respective banks which is a key matter of concern. Every bank in India must ensure that they either frequently or quarterly arrange various cybersecurity awareness programs or workshops so that the rate of awareness gets higher among the users.

Question 18. How often do you think users should be educated about the latest cybersecurity threats in online banking?

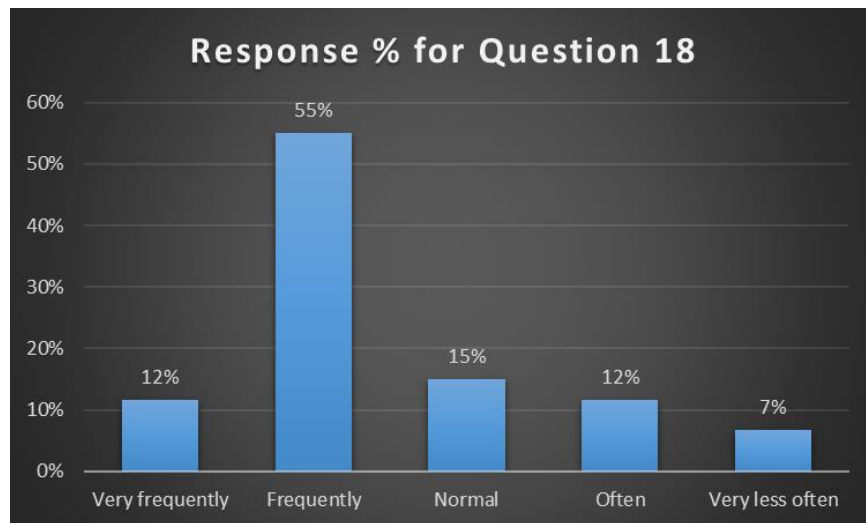


Figure 4.18 Respondents response for question 18

(Source: Created by researcher)

This interpretation concludes that the majority of the respondents should be educated by the financial institutions or banks about the latest cyber security threats in online banking platforms. They need to be aware of this because, although there are a lot of security solutions available that offer an important level of safeguarding, such safeguards may not be effective without user awareness. Moreover, schooling for these users in India includes disseminating information and understanding possible risks, security standards, and methods to detect and prevent them.

Question 19. How far do you agree that the current strategies in place effectively mitigate the risks of identity theft in online banking?

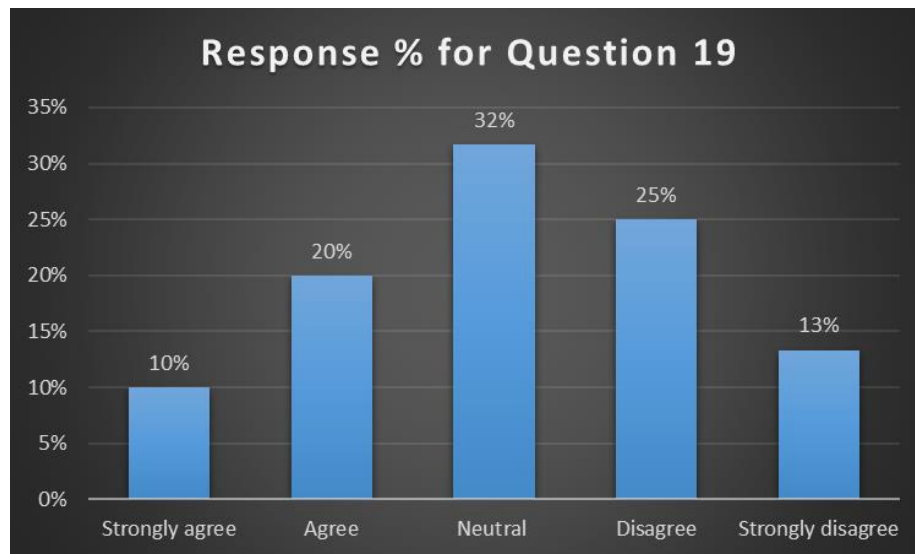


Figure 4.19 Respondents response for question 19

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of the respondents disagree with this question. In other words, it can be derived from the respondent's response that current strategies in place are not effective enough in mitigating the risk of identity theft in online banking. The rate of disagreement also indicates that many of the respondents are not happy or satisfied with the current strategies in place that effectively mitigate the risks of identity theft in online banking. It can be added that due to the evolving landscape of digital processes, novel approaches must be developed and implemented to guarantee user account security by identifying theft in online banking platforms.

Question 20. How would you rate the level of awareness regarding cybersecurity among your peers?

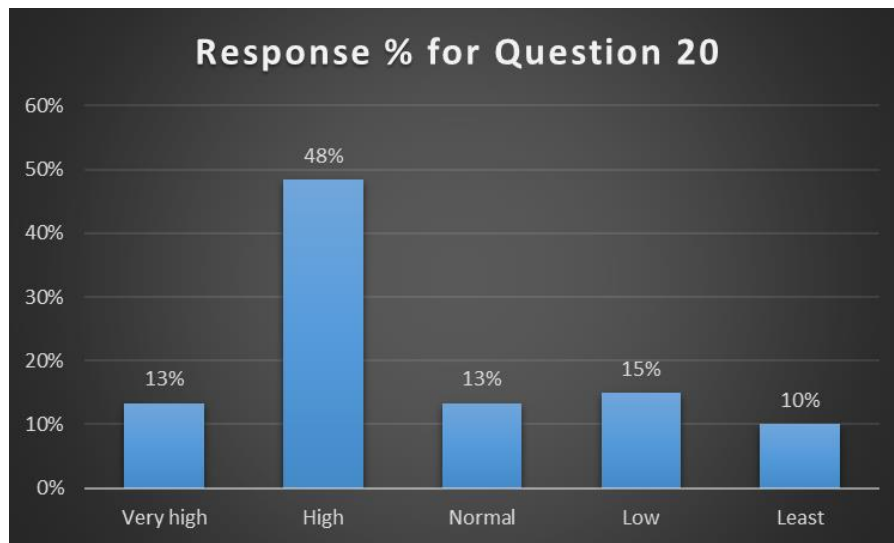


Figure 4.20 Respondents response for question 20

(Source: Created by researcher)

From this interpretation, it can be said that the majority of their peer's awareness regarding cyber security is high. In contrast, a few respondents have raised concerns about this matter which indicates that the level of awareness regarding cybersecurity among their peers is not good enough. This indicates that better judgement and seriousness are required to enhance the level of awareness.

Question 21. How often do you receive information or support from your bank regarding online security?

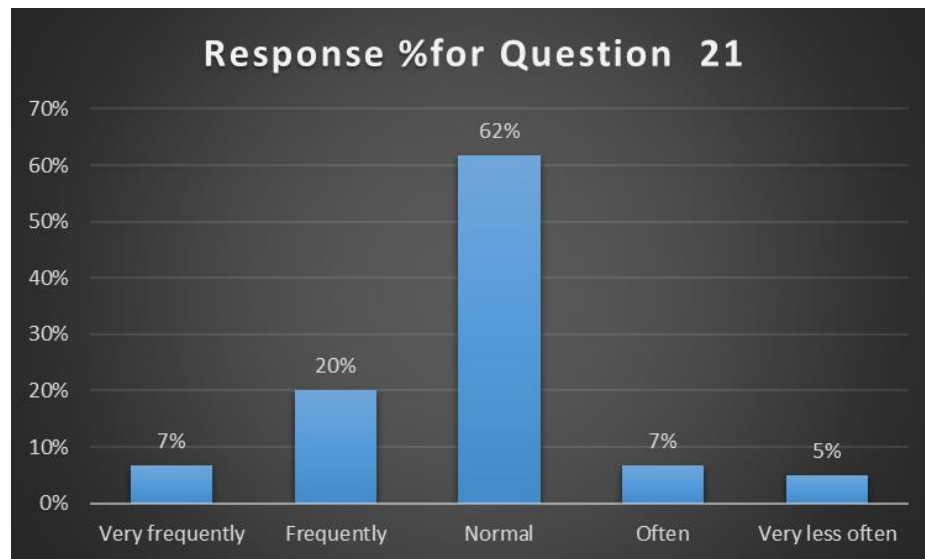


Figure 4.21 Respondents response for question 21

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of them sometimes get or do not get any information or support from their respective bank regarding online security. It is a matter of concern that 62% of the respondents have stated “Normal”. In a developing country like India, it is not appreciable. There are multiple banks in India and it is their moral and legal duty to notify users about online security and also provide support. Banking institutions must keep an eye on this and Indians must be aware of this matter so that they can charge the banks against such serious matters.

Question 22. Would you be willing to recommend specific strategies to others for mitigating online banking fraud and identity theft?

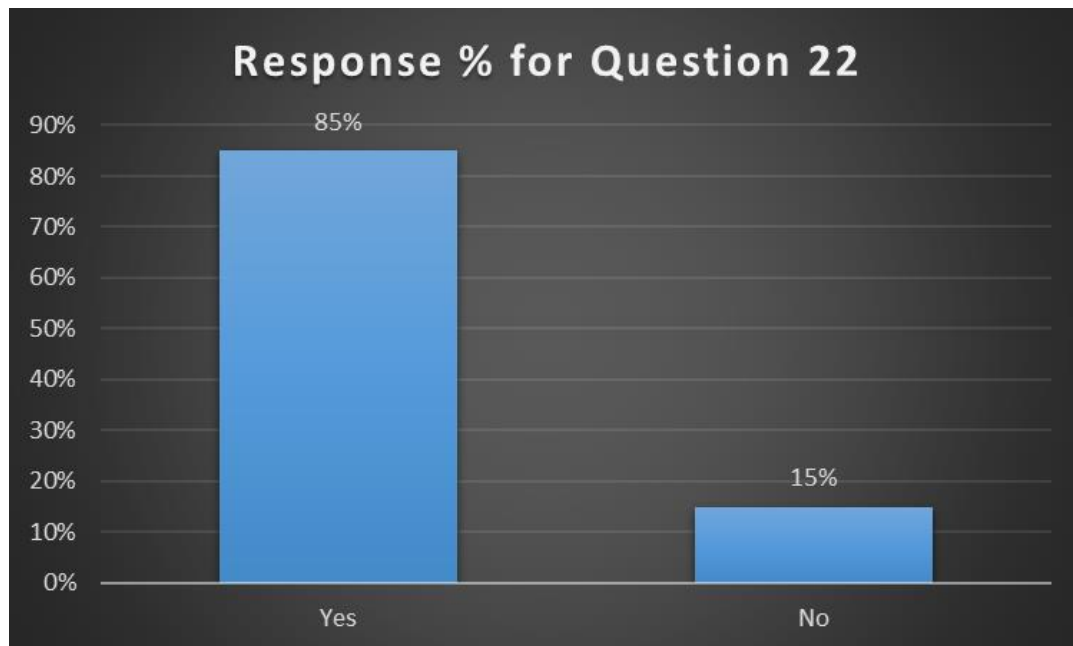


Figure 4.22 Respondents response for question 22

(Source: Created by researcher)

This interpretation concludes that the majority of the respondents are willing to recommend strategies to others to mitigate online banking fraud and identify theft. It indicates that people care for others' well-being and safety. As the researcher has already mentioned once in India people care about their money and that is why they are becoming more serious and conscious about online banking processes. This seriousness plays a key role in ensuring that a user's account and also others' accounts are safe as they are ready to suggest specific strategies to mitigate online banking fraud and identity theft.

Question 23. How far do you think financial institutions provide sufficient information and support regarding online security?

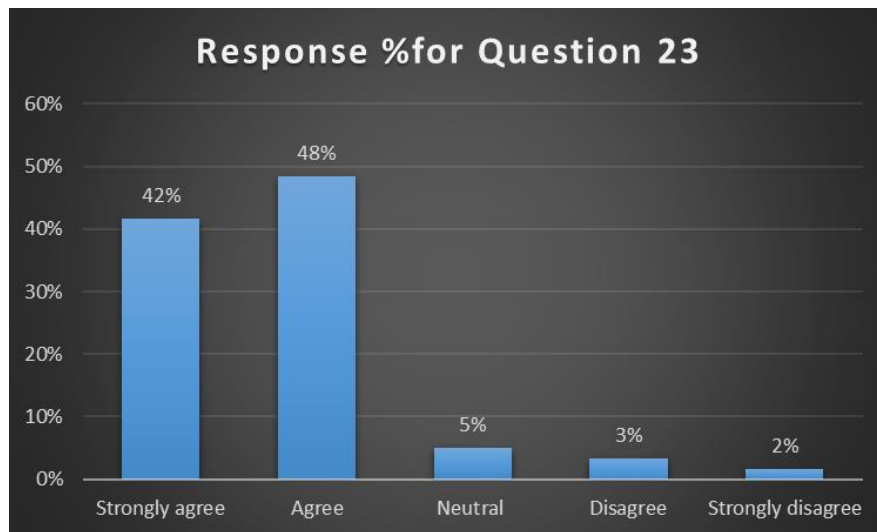


Figure 4.23 Respondents response for question 23

(Source: Created by researcher)

This interpretation concludes that the majority of the respondents responded that financial institutions are providing sufficient information and support regarding online security. The positive response indicates that the financial institutions are performing their job nicely in this developing nation as they have understood that sharing is caring and that is how they can battle against online fraud and scams. Such things also help users to build trust in the financial institutions and their mental well-being does not hit negatively and stays stable.

Question 24. How secure do you feel when conducting online banking transactions?

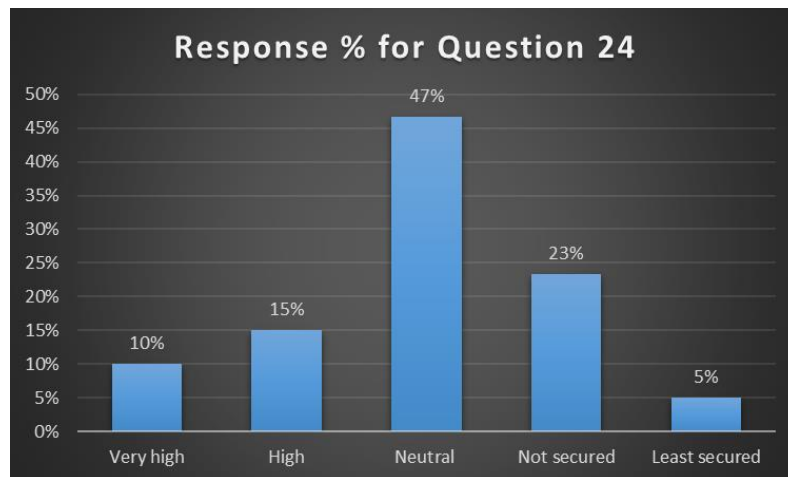


Figure 4.24 Respondents response for question 24

(Source: Created by researcher)

From this interpretation, it can be concluded that the majority of the respondents are not sure that they feel secure or not secure, due to cyber security issues in online banking platforms. It can be added that there are many things to do to improve this nasty and detrimental situation. Not feeling comfortable is a key concern and staying neutral in an interview process is another matter of concern. The banking sector must do something so that people in India feel confident and secure while making online transactions. Staying neutral does not highlight the positive sides of the matter.

Question 25. Based on your experiences, do you have specific recommendations for improving online banking security?

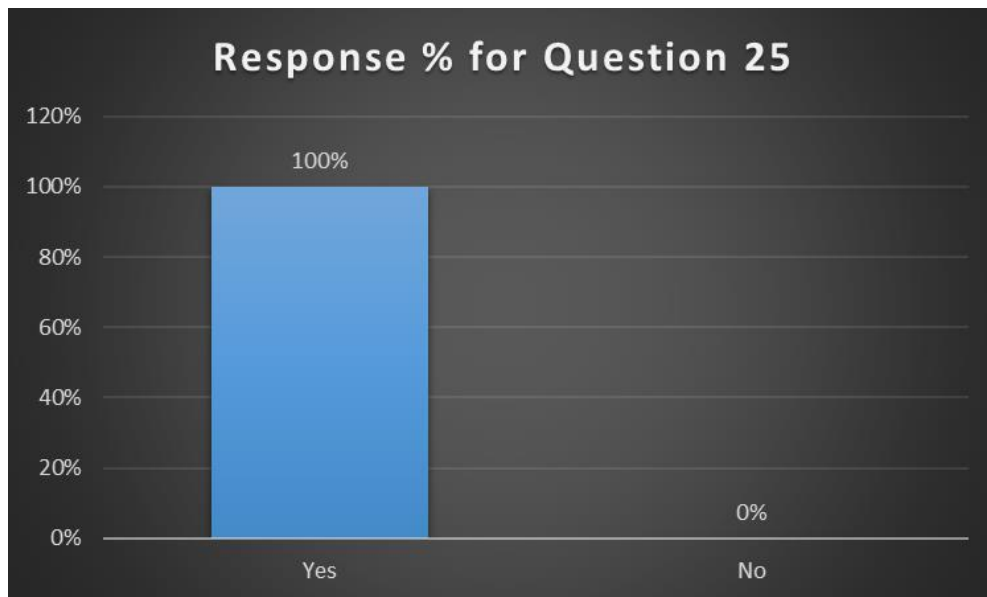


Figure 4.25 Respondents response for question 25

(Source: Created by researcher)

This interpretation helps to conclude that all the respondents believe that based on their experience with online banking security, they can provide a few recommendations which can help in improving online banking security. In this regard, they can go for different strategies like frequently changing passwords and login details, not clicking on any spam links or even they must not share their login details with any third-party entities. Having licensed anti-virus software is always useful. Both the users and banking institutions in India must work collaboratively to stop fraud and detect internet theft to apply protective measures.

4.4 Discussion and Findings

In this section of the chapter, the overall findings of the study described in the previous section has been analysed. Whenever one considers the whole expansion of Internet banking in India over the past several decades, one finds that the process has been quite transformational. Due to several causes, including the growing usage of smartphones, improved accessibility to the Internet, and government initiatives to promote a digital economy, online banking has emerged as a critical component of the financial landscape. Users can simply manage accounts they have, conduct activities, and pay their financial obligations from the security of their own homes with the use of Internet connections.

In the above part of this chapter, all the responses of the respondents are presented and analysed to drive the possible solutions of this study. Based on the responses of the respondents, a broad discussion is presented by a researcher to analyse the issues critically and illustrate possible strategies that could mitigate the issues. From the respondent's responses, it can be said that the majority of the respondents of the study have faced fraudulent activities frequently while opting for online banking activities. Despite financial institutions or banks implementing strategies and raising awareness of cyber security and thefts, these issues are increasing day after day. It was also observed that users and customers are opting for better cyber security measures but still, the issues prevail.

Internet banking transactions are a blessing for consumers in today's fast-paced world, but the rising number of scams and thefts has made them a scourge. Customers and users who have already experienced similar problems find it impossible to trust this online means of transaction. They are dissatisfied and concur with the infrastructure put in place by the banking industry to thwart fraud and theft as users and clients of the relevant bank. By helping customers and teaching them about internet transactions, banks are refining their approach. Cybercriminals use cutting-edge tactics and technologies that are impossible for users to stay aware of or keep up to speed with. Because of the inadequate financial methods and infrastructure, cybercriminals are growing more unstoppable. This is the main leading reason behind the few customers are not users of online banking platforms and prefer old banking transactions.

Because they are incapable of keeping up with the innovations in technology, customers still choose classic Internet banking services over more recent mobile banking services. Various monetary firms are unable to supply them with the technological resources that would enable

them to create code and hardware that is impervious to hackers and capable of identifying illicit activity. Whereas, the literature review segment has illustrated some key in Internet Banking and also has discussed the fraudulent activities cases in India which makes this matter more concerning and critical. It is possible to argue that banks may educate the public about specific steps that must be taken to eradicate deception, however regular training sessions as well as educational initiatives are extremely uncommon. The sole strategy for creditors to lessen such challenges has been to set up informative events and advertisements that will aid in the consumers' and clients' learning and development. The literature review segment has also mentioned about level of awareness and education about this matter which confirms that training sessions are highly required here. Such training sessions need to be sufficiently successful in imparting knowledge on all procedures, including password changes, software updates, and several safeguards against the loss of private data and banking transactions. In the suggestions section of the dissertation's last chapter, there is a further treatment of this topic. Moreover, before that it is also important to gather data about various types of fraudulent activities that are present in India and the literature review chapter has shed light on this matter as well.

A large proportion of those surveyed said in their comments that they got phishing notifications and texts on their enrolled personal contact details. Users are nonetheless uneasy employing online financial transaction techniques even after they have changed the usernames and privacy preferences on their web-based financial profiles. Additionally, this material is of great significance considering that it is covered in the literature review section. Phishing assaults, stolen identities, and online viruses all pose serious risks that need major expenditures in high-tech cybersecurity measures to secure sensitive customer data. While making comparison, it can be claimed that ensuring the safety of individual knowledge and digital payments involves an ongoing problem that demands perpetual creativity as well as inspection. These respondents are willing to use a two-step authentication process for better and safer online transactions. In other words, it can be said that users are not confident enough in using modern online banking facilities despite all prevention. It is necessary that implementing a two-step authentication process and other safe money transfer methods by the banks is necessary. Enhancing privacy is of utmost importance in online banking. Financial institutions can use state-of-the-art fingerprint authorization systems if they recognize this. Technology for fingerprinting and face recognition allows for complex security, enhancing the defence against unauthorized access to sensitive user data.

Online financial services appear to benefit greatly from the application of various technological advancements such as machine learning and AI. Such systems have the ability to go across enormous amounts of data and examine user behaviour to find abnormalities that might signify an intrusion operation. Data of this dissertation reflects that AI's adaptability allows it to continuously improve, preventing new attacks and strengthening the defence mechanism. Adopting artificial intelligence (AI) and machine learning (ML) seems to be a crucial strategy for bolstering online banking systems, as the literature review section has shown. It is also obvious that banks are using AI-enabled apps and virtual assistants driven by AI to improve client happiness. In terms of using technology, the literature review has also agreed on this and has mentioned about the usefulness of blockchain technology in cybersecurity management in the banks and financial institutions. Blockchain technology is beginning to emerge as a groundbreaking remedy for issues with data transparency as well as trustworthiness. Moreover, it uses the fragmented trace of operations to construct an immutable database. It is arguably true that this increases trust in the dependability of investments while also reducing the possibility of mistakes as well as frauds.

Users from heavily populated regions of India, such as big cities, should be informed about all the cyber security precautions linked to fraudulent activity. This is required to stop thefts, spread knowledge about them, and provide safety measures for users and residents in densely populated places against fraud. It may be concluded from the research respondents' readiness to participate in the study that other users, who did not participate in the study, are also eager to adopt and comprehend the use of specific cyber security measures. This is encouraging since it will enable banks and other financial organisations to achieve their cybersecurity goals and stop fraud and theft.

The financial services industry must use modern technologies and a variety of ways to connect in addition to strengthening security protocols and creating networks to raise public knowledge of online thefts alongside the steps taken to avoid them. Since the literature review revealed that there are numerous ways to obtain data and cause harm to financial institutions, banks must regularly raise user knowledge and consciousness to continue keeping users informed about intriguing updates and technological advances, and what to do to avoid problems down the road. The greatest percentage of participants also endorse this, demonstrating how crucial it is to improve cybersecurity for India's banking industry. Moreover, as per the respondent's responses, banks are providing frequent education workshops for their users and the majority of these respondents have visited. In this same context, other users are also invited by the banks

to visit these workshops but the rest of the users are not able to attend these workshops are facing issues. The rest of the users are not aware of the usage and prevention methods implemented by their respective banks. However, in this regard, the literature review lacks data which indicates that further research on this field needs to be done in future. Hence, banks and other financial institutions need to develop certain communication modes or channels which will help them spread information to all those users who are not aware of the measures. This will lead to a decrease in the occurrence of fraudulent activities as the more than majority of users are getting informed and aware by the banks and several financial institutions.

Apart from the financial losses, users are having a hard time in the behavioural and psychological aspects of their own lives. During the survey interview questionnaire method, respondents were asked about the psychological and behavioural impact of thefts and fraudulent activities. The majority of the respondent's responses were yes. From these responses, it can be stated that fraudulent activities are also impacting the lifestyle and psychological well-being of the users. In future, it may lead to a prominent reason behind stopping using modern Internet banking by the users. Respondents believe that strategies and measures especially in-place strategies are not capable of mitigating the risk of fraudulent activities and threats related to online money transfers. Such data is quite significant as the financial losses not only hamper the financial stability of the victims but also impact the psychological wellness of them which can trigger the behavioural changes. The literature has talked about number of internet banking fraudulent activities cases in India, however, it does not indicated any suitable solution apart from the application of modern technologies. Therefore, a key insight on this regard is reflected in the recommendations segment to fill this gap.

Due to the lack of support and feedback asked from their users, financial institutions and banks might face trouble dealing with online banking fraudulent activities. The literature review has mentioned that Indian users are not so smart and active so that they can raise quire to their respective banks about their account safety and safe online transactions. This is where the main concern rises in India about cybersecurity. However, it is also necessary that banks ask or rely on their users to deliver their unbiased opinions and maintain healthy communication. It is the duty and responsibility of banks and other financial institutions to educate their users and customers and inform them about all the negative impacts they are likely to face. Banks and financial institutions that are incorporating online banking transactions need to establish customer grievances cells where all the issues feedback and complaints of the customers will

be analysed and effective advice will be provided to their customers in return. Without developing healthy relations or providing assistance after fraudulent activities and thefts, it is banks' and financial institutions' responsibility to help their users.

With the help of survey result it can be claimed that various monetary organisations in India do ask any information and ideas from their customers or users. This holds a large communications gap and technological gap with the customers and companies that hackers are building and in return, they benefit from these gaps. Moreover, the literature review segment has talked about various types of fraudulent activities in India which shows a key concern for the users in this nation. Without frequent interactions, fewer educational workshops, and avoiding the majority of the busy areas in India to name a few fraudulent activities are increasing in India. This indicates that some supportive role from both the end is highly essential so that cybersecurity can be improved and number of fraudulent activities will get deteriorate in India. This has forced the researcher to make recommendations to bridge this gap and improve the situation which is conducted in the next chapter of this dissertation.

4.5 Conclusion

From the above discussion it can be understood that, in this chapter, the researcher is presenting all the data and information collected from their survey method. Researchers have implemented the quantitative analysis method through the graphical representation method. At the beginning of this chapter, the researcher represents the data collected from the 60 respondents through graphical representation and short illustrations are given. In the second part of this chapter, the researcher discussed all the important aspects that were observed from the data collection. This part holds an overall discussion and analysis of the aspects for which this study was conducted to derive favourable solutions to the problem statement of this study. In the next chapter of this study, which is the last chapter, the researcher provides a few recommendations along with a conclusion. Other than these limitations and future scope of the study are also discussed providing the linking with the objectives of the study for a better understanding of the outcome of the study.

Chapter 5. Conclusion and Recommendation

5.1 Summary

It has been determined from the evaluation above section that online banking services have grown considerably in India. However, it has also been discovered that there are a lot of significant issues with digitalization in the banking sector. To guarantee the dependability, stability, and credibility of the nation's whole banking sector, these issues demand serious consideration. Since there are more online transactions, there is also a greater chance of cyber threats including virus attacks, phishing scams, and theft of identities. For this reason, cyber safety represents several of the most important issues. Consequently, bankers need to constantly make investments in a solid security ecosystem in order to protect client data and monetary transactions from unauthorized entry and malicious activity. Improved consumer understanding and proficiency with technology are two more important issues with online banking.

To foster reliability and guarantee widespread acceptance, it is crucial to make arrangements that the programs are concentrated on teaching users about safe online behaviour, spotting fraudulent transactions, and comprehending the safeguarding layouts of banking services. Another significant worry is flexibility in operation since it could lead to issues during the event of a system breakdown or technical difficulties. In addition to this, managing consumer data as well as determining if it is susceptible to unauthorized access raises serious issues regarding confidentiality. Therefore, it's critical to establish trust amongst Internet banking consumers through stringent privacy regulations and transparent banking communications concerning their confidential practices.

A further significant problem facing the online financial services sector is regulations. It is imperative to keep an effective equilibrium between innovations and adherence to regulation norms. It is a significant obstacle, though. Therefore, to preserve the integrity of digital banking services, it is necessary to enact flexible laws that keep up with developments in technology while safeguarding customer interests and the financial system. In the end, it has been concluded that resolving privacy concerns, raising user knowledge, maintaining flexibility in operations, safeguarding confidentiality, and guiding regulatory hurdles are critical elements that can assist in resolving difficulties with India's Internet banking industry. A concentrated

effort by financial institutions authorities, and government officials is necessary to build a robust and safe digital financial environment that offers substantial advantages to all clients.

In the above chapters, it is described and analysed effectively about all the loopholes and gaps that are between the users of banks and financial institutions. Researchers have presented the 60 respondents' data from the survey questionnaire method, and based on that analysis few recommendations will be provided and a conclusion will be discussed. It was observed that theft of frauds and loss of money during online banking transactions of the users are impacting both psychological and behavioural aspects of their lives adversely. It is also analysed that financial institutions and banks are providing very little assistance and support to their users and very few times messages as well as notifications regarding security breaches are provided.

This highlights the communication gap between the customers and the company. Other than this gap, there is a huge gap that this bank needs to fill which is the technology gap. Banks might be spreading enough advertisement and training through workshops but these facilities are not so frequent. Due to this reason, users are not aware of the latest technology implemented by the banks and ways to operate this technology effectively. Respondents who are users feel that banks need to develop their in-place strategies, and infrastructure and also allow feedback from the users and provide support assistance to them which will develop the technology and be more effective in developing online banking transactions safe from theft.

5.2 Linking objectives with the study

Objective 1. To inspect the strategies implemented by cyber-attackers in India

Based on the data analysis, it can be concluded that cyber attackers in India are implementing technology far more advanced than the banks. This is one of the most common reasons why banks are unable to stop fraudulent activities. Cyber-attackers are taking advantage of the communication gap and technology gap between the company which is banks and users which is resulting in leaking private information related to online bank transactions. Hackers are updating their technology way more than financial institutions which is impacting the banks in establishing the ideal infrastructure which will help them secure the data and information of the users and safeguard them from theft.

Objective 2. To find out the impact of cyber threats on psychological as well as behavioural aspects of individuals in India

Due to the rise in cyber threats in India, it was observed that respondents do face issues with psychological and behavioural aspects in their daily lives. This causes severe issues in their health as theft of losing money is haunting users of online banking transactions. Banks are providing a few workshops and educational messages but these are very less frequent which does not allow the users to know about the latest technology that is ongoing in the market. Due to a lack of information and the idea of using technology, hackers are utilising this technological gap to fraudulent money in transactions harming the users in their respective lives.

Objective 3. To find out the risks linked with mobile banking and online banking

As per the data withdrawn from the respondents of this study, it can be stated that the majority of the users choose traditional online banking rather than mobile banking. It is because it is easy for hackers to get information about the user's personal information like sim card numbers, mobile numbers, email IDs and passwords, even if users are changing the security settings. This is one of the main reasons, cyber-attackers are able to hack their personal information and also send them phishing or other emails and messages as a trap to hack their online bank accounts. This is a major drawback that is impacting the users in preventing their data from getting leaked to safeguard their online bank accounts.

5.3 Recommendation

On the basis of data collection from the participants of this study, data analysis is made. On this data collection and observation, a few recommendations will be discussed below to prevent future fraudulent issues and mitigate the risk of threats for the users of online bank transactions.

- **Building trust issues of the users or the customers:** Fraudulent activities lead to impact the trust issues of the users and customers. After these frauds and thefts, they have a hard time trusting the bank and its financial system. Banks need to develop their relation with their customers and help them in all possible means retrieving all their lost money and protecting their privacy. In some cases, there are customers whose issues were not solved by the banking department. Banks need to focus on making their relationship better with their customers and implement new management systems that develop the technology and ensure the privacy and security of the data of the users.
- **Provide training and increase awareness of the cyber security measures-** it is important for the banking system to provide necessary training or education facilities

to the users of their online banking transactions. This will lead to educating the users in using the application and system in a better way. This also prevents users from maintaining the privacy of their personal information on those accounts and prevents them from leaking to the cyber-attackers. On the other hand, increasing the awareness of fraud will help in spreading all the measures which are necessary for mitigating the issues related to cyber threats.

- **Developing the relationship with the users-** banks and other financial systems need to develop a positive relationship with their customers to develop their business and prevent losing any customers or users in future. This will benefit the banks in providing better services to their users after receiving feedback and suggestions regarding developing the technology. When users are connected and well assisted by the users, they will feel they are part of the company. This will induce a positive mindset among the users which will help them in combating their psychological and behavioural issues.

5.4 Limitations of Study

Many challenges confronted this investigator throughout this investigation. The investigator had to face many challenges to complete this research project and to collect and analyze the data. The objectives of the study were not tailored to the company; instead, they were meant to offer a general assessment, and the representative group that was selected for data gathering was inadequate. In this case, those who responded took a while to provide their responses. Furthermore, the investigator could not obtain supplementary facts and data sources that would have impacted the results of feasible strategies for multinational enterprises.

5.5 Future Scope of Study

In this research, researchers have implemented primary data from the users of online banking in India. For vivid discussion, researchers need to analyse the strategies and issues that professionals face while incorporating technology upgrades to prevent cyber attacks. In future, researchers might analyse the viewpoints and challenges of the professionals working in banks and financial systems which will provide a broad idea about the working to prevent cyber attacks. Other than these aspects, international banking systems are implementing effective technology to prevent these cyber issues. This is also another aspect that needs to be analysed or compared with the Indian infrastructure implemented by the bank. This will lead to sketching huge landscapes about the cyber security prevention measures in future.

References

- Acharya, S. and Joshi, S., (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. *PalArch's Journal of Archaeology of Egypt/Egyptology*, 17(6), pp.4656-4670.
- Al-Ababneh, M., (2020). Linking ontology, epistemology and research methodology. *Science & Philosophy*, 8(1), pp.75-91.
- Ali, L., (2019). Cyber crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC). *The Journal of Developing Areas*, 53(1).
- Babii, A., (2020). Important aspects of the experimental research methodology. *Вісник Тернопільського національного технічного університету*, 97(1), pp.77-87.
- Banu, A.M., Mohamed, N.S. and Parayitam, S., (2019). Online banking and customer satisfaction: evidence from India. *Asia-Pacific Journal of Management Research and Innovation*, 15(1-2), pp.68-80.
- Budianto, A., (2020). Legal research methodology reposition in research on social science. *International Journal of Criminology and Sociology*, 9(1), pp.1339-1346.
- Carbo-Valverde, S., Cuadros-Solas, P. and Rodríguez-Fernández, F., (2020). A machine learning approach to the digitalization of bank customers: Evidence from random and causal forests. *Plos one*, 15(10), p.e0240362.
- D'Silva, D., Filková, Z., Packer, F. and Tiwari, S., (2019). The design of digital financial infrastructure: lessons from India. *BIS Paper*, (106).
- Datta, P., Tanwar, S., Panda, S.N. and Rana, A., (2020, June). Security and issues of M-Banking: A technical report. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1115-1118). IEEE.
- Dey, K.A., (2019). *Mitigation of Identity Theft in Online Banking* (Master's thesis, The University of Bergen).
- Dodds, S. and Hess, A.C., (2020). Adapting research methodology during COVID-19: lessons for transformative service research. *Journal of Service Management*, 32(2), pp.203-217.

Bhatnagar, V. and Mishra, N., (2019). Perspective on Prevalent Banking/ATM Frauds Focused on Types of Frauds, Methodologies Adopted And Suggested Preventive Measures/Solutions..

SINGH, I., NAYYAR, A., LE, D.H. and DAS, S., (2019). A conceptual analysis of internet banking users' perceptions. An Indian perceptive. *Revista Espacios*, 40(14).

Dzwigol, H., (2022). Research methodology in management science: Triangulation. *Virtual Economics*, 5(1), pp. 78-93.

Firdaus, F., Zulfadilla, Z. and Caniago, F., (2021). Research methodology: Types in the new perspective. *Manazhim*, 3(1), pp.1-16.

Gayan Nayanajith, D.A. and Damunupola, K.A., (2019). Effects of Subjective Norms and Security on Online Banking Adoption: Multilevel Linear Model Analysis. *Asian Journal of Multidisciplinary Studies*, 1(1), pp.9-16.

Ghelani, D., Hua, T.K. and Koduru, S.K.R., (2022). A Model-Driven Approach for Online Banking Application Using AngularJS Framework. *American Journal of Information Science and Technology*, 6(3), pp.52-63.

Ghosh, U., (2021). Online financial frauds and cyber laws in India-an analysis. *FINANCIAL FRAUDS AND CYBER LAWS*, , Issue 10.

Greening, N., (2019). Phenomenological research methodology. *Scientific Research Journal*, 7(5), pp. 88-92.

Gupta, R., Gupta, S. and Ajekwe, C.C.M., 2023. Electronic Banking Frauds: The Case of India. In *Theory and Practice of Illegitimate Finance* (pp. 166-183). IGI Global.

Haralayya, B. and Aithal, P.S., 2021. A Study On Structure and Growth of Banking Industry in India. *International Journal of Research in Engineering, Science and Management*, 4(5), pp.225-230.

HR, G. and Aithal, P.S., 2022. The DDLR model of research process for designing robust and realizable research methodology during ph. d. program in India. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 7(2), pp.400-417.

Hughes, M. and Barlo, S., 2021. Yarning with country: An indigenist research methodology. *Qualitative inquiry*, 27(3-4), pp.353-363.

Ibrahim, U., (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. *NDIC Quarterly*, 34(12), pp. 1-20.

Jibril, A.B., Kwarteng, M.A., Botchway, R.K., Bode, J. and Chovancova, M., 2020. The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, 7(1), p.1832825.

Jibril, A.B., Kwarteng, M.A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M. and Chovancova, M., 2020, April. Online identity theft on consumer purchase intention: A mediating role of online security and privacy concern. In *Conference on E-Business, e-Services and e-Society* (pp. 147-158). Cham: Springer International Publishing.

Kaur, S. and Arora, S., 2020. Role of perceived risk in online banking and its impact on behavioral intention: trust as a moderator. *Journal of Asia Business Studies*, 15(1), pp.1-30.

Kaur, S.J., Ali, L., Hassan, M.K. and Al-Emran, M., 2021. Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, 26, pp.107-121.

Kitsios, F., Giatsidis, I. and Kamariotou, M., 2021. Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(3), p.204.

KOTTECHA, D., (2019). Growth and Trends of Mobile Banking in India.. *International Journal for Research in Management and Pharmacy*. , 8(4), pp. 28-30.

Leonardo Cavaliere, L.P., Subhash, N., Durga Rao, P.V., Mittal, P., Koti, K., Chakravarthi, M.K., Duraipandian, R., Rajest, S.S. and Regin, R., 2021. The Impact of Internet Fraud on Financial Performance of Banks. *Turkish Online Journal of Qualitative Inquiry*, 12(6).

Lin, W.R., Wang, Y.H. and Hung, Y.M., 2020. Analyzing the factors influencing adoption intention of internet banking: Applying DEMATEL-ANP-SEM approach. *Plos one*, 15(2), p.e0227852.

Mahuika, N. and Mahuika, R., 2020. Wānanga as a research methodology. *ALTERNATIVE: An international journal of indigenous peoples*, 16(4), pp.369-377.

Manoharan, S., Katuk, N., Hassan, S. and Ahmad, R., 2022. To click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, 30(1), pp.37-62.

- Manoj, K., (2021). Cyber risk in banking services: the extent of cyber risks provisions and security measures. *International Journal of Management (IJM)*, 12(1), pp. 1332-1339.
- Mawgoud, A.A. and Ali, I., 2020, February. Statistical insights and fraud techniques for telecommunications sector in Egypt. In *2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)* (pp. 143-150). IEEE.
- Naeem, M. and Ozuem, W., 2021. The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services*, 60, p.102483.
- Newman, M. a. G. D., (2020). Systematic reviews in educational research: Methodology, perspectives and application.. *Systematic reviews in educational research: Methodology, perspectives and application*, pp. 3-22.
- Niemand, T. R. J. K. A. K. S. a. M. A., (2021). Digitalization in the financial industry: A contingency approach of entrepreneurial orientation and strategic vision on digitalization.. *European Management Journal*, 39(3), pp. 317-326.
- Nwarize, C., (2023). An investigation of factors influencing non-users' resistance to internet banking adoption in Nigeria. (*Doctoral dissertation, Cardiff Metropolitan University*)..
- Ocaña-Fernández, Y. and Fuster-Guillén, D., 2021. The bibliographical review as a research methodology. *Revista Tempos E Espaços Em Educação*, 14(33), pp.e15614-e15614..
- Patel, M. a. P. N., (2019). Exploring research methodology. *International Journal of Research and Review*, 6(3), pp. 48-55.
- Pazarbasioglu, C. M. A. U. M. N. H. F. E. a. S. M., (2020). Digital financial services. *World Bank*, Volume 54.
- Rahi, S., Mansour, M.M.O., Alghizzawi, M. and Alnaser, F.M., 2019. Integration of UTAUT model in internet banking adoption context: The mediating role of performance expectancy and effort expectancy. *Journal of Research in Interactive Marketing*, 13(3), pp.411-435.
- Rajasinghe, D., 2020. Interpretative phenomenological analysis (IPA) as a coaching research methodology. *Coaching: An International Journal of Theory, Research and Practice*, 13(2), pp.176-190.

- Reddy, C., (2020). Teaching research methodology: Everything's a case.. *Electronic Journal of Business Research Methods*, 18(2), pp. 178-188.
- Reynolds, D., (2022). Identity Theft Victims' Understandings of Incidents and their Reporting Decisions. *Doctoral dissertation, University of Guelph*.
- Rouge, P., Yeung, C., Salsburg, D. and Calandrino, J.A., 2020. Checkout checkup: Misuse of payment data from web skimming..
- Ryder, C., Mackean, T., Coombs, J., Williams, H., Hunter, K., Holland, A.J. and Ivers, R.Q., 2020. Indigenous research methodology—weaving a research interface. *International Journal of Social Research Methodology*, 23(3), pp.255-267.
- Sarjiyus, O., Oye, N.D. and Baha, B.Y., 2019. Improved online security framework for e-banking services in Nigeria: A real world perspective. *Journal of Scientific Research and Reports*, 23(1), pp.1-14.
- Shaaban, R., (2020). Factors influencing the use of electronic payment system among the bank customers: a case study of NMB bank. *Doctoral dissertation, Mzumbe University*.
- Shankar, A. and Jebarajakirthy, C., 2019. The influence of e-banking service quality on customer loyalty: A moderated mediation approach. *International Journal of Bank Marketing*, 37(5), pp.1119-1142.
- Shaw, P. and Saha, S.K., 2020. OPPORTUNITIES AND CHALLENGES OF DIGITALIZATION IN THE BANKING SECTOR: AN EMPIRICAL STUDY ON CUSTOMER'S ATTITUDE AND PERCEPTION TOWARDS ONLINE BANKING IN DARJEELING DISTRICT. *Jamshedpur Research Review*..
- Singh, S., (2019). Measuring E-service quality and customer satisfaction with internet banking in India. *Theoretical Economics Letters*, 9(2), pp. 308-326.
- Suryono, R., (2020). Challenges and trends of financial technology (Fintech): a systematic literature review. *Information*, 11(12), pp. 590.
- Tajpour, A., (2020). Identity Theft and Prevention. *Information Security and Optimization*., pp. 25-42.
- Tick, (2021). Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19.. *Electronics*, 10(22), p. 2865.

TODAY, I., (2023). *Senior citizen loses Rs 8.3 lakh while shopping for towels online, full story..* [Online]

Available at: <https://www.indiatoday.in/technology/news/story/software-engineer-loses-more-than-rs-2-lakh-while-booking-cab-online-here-is-what-happened-2332126-2023-02-08>

[Accessed 25 November 2023].

Verma, (2020). Antecedents of online banking adoption: An empirical study in an emerging economy.. *Journal of Services Research*, 20(1/2), pp. 7-19.

Vig, (2022). Customer Perception Towards Online Banking.. *Proceedings of the International Conference on Advances in Management Practices (ICAMP 2021)*..

Vishnuvardhan, B., Manjula, B. and Lakshman Naik, R., (2020). A study of digital banking: Security issues and challenges.. *In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018*, pp. 163-185.

Yildirim, N. and Varol, A., (2019). A research on security vulnerabilities in online and mobile banking systems.. *In 2019 7th International Symposium on Digital Forensics and Security (ISDFS)* , pp. 1-5.

Appendix

Survey Questionnaire

1. How frequently have you encountered fraudulent activities in your internet banking transactions?

- a. Very frequently
- b. Frequently
- c. Normal
- d. Often
- e. Very often

2. How far do you agree that current online banking infrastructure effectively addresses the level of fraudulent activities?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

3. Have you ever personally experienced vulnerabilities in the security of your online banking platform?

- a. yes
- b. No

4. How far do you think cyber-attackers have become more sophisticated in their strategies over the past few years?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

5. To what extent do you believe cyber threats can impact the psychological well-being of individuals using online banking?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Disagree

6. How far do you agree that there are specific risks associated with mobile banking compared to traditional online banking?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

7. how would you rate your awareness of cybersecurity practices related to online banking?

- a. Excellent
- b. Very good
- c. Good
- d. Bad
- e. Worst

8. How frequently do you update your passwords and security settings for your internet banking accounts?

- a. Very frequently
- b. Frequently
- c. Normal
- d. Often
- e. Very often

9. How far do you think there is sufficient awareness about cybersecurity among users in densely populated areas?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

10. Would you be open to using additional security measures, such as two-factor authentication, for online banking?

a. Yes

b. no

11. How confident are you in recognizing and avoiding potential cyber threats in online banking?

a. Highly confident

b. Confident

c. Neutral

d. Less confident

e. Least confident

12. Have you ever received phishing emails or messages related to your online banking account?

a. Yes

b. No

13. How often do you think financial institutions should provide updates or notifications regarding cybersecurity measures?

a. Very frequently

- b. Frequently
- c. Normal
- d. Often
- e. Less often

14. How far do you believe there is a need for increased education and awareness about online banking security?

- a. Highly agree
- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

15. how would you rate the impact of cyber threats on your behavioral aspects related to online banking?

- a. Highly significant
- b. Significant
- c. Neutral
- d. Not significant
- e. Least significant

16. How far are you satisfied with the strategies implemented by your online banking provider to prevent cyber-attacks?

- a. Highly satisfied
- b. Satisfied
- c. Neutral
- d. Dissatisfied
- e. Highly dissatisfied

17. Have you attended any cybersecurity awareness programs or workshops provided by your bank?

- a. Yes
- b. no

18. How often do you think users should be educated about the latest cybersecurity threats in online banking?

- a. Very frequently
- b. Frequently
- c. Normal
- d. Often
- e. Very often

19. How far do you agree that the current strategies in place effectively mitigate the risks of identity theft in online banking?

- a. Highly agree

- b. Agree
- c. Neutral
- d. Disagree
- e. Highly disagree

20. how would you rate the level of awareness regarding cybersecurity among your peers?

- a. Very high
- b. High
- c. Normal
- D. Low
- e. Least

21. How often do you receive information or support from your bank regarding online security?

- a. Very frequently
- b. Frequently
- c. Normal
- d. Often
- e. Very often

22. Would you be willing to recommend specific strategies to others for mitigating online banking fraud and identity theft?

- a. Yes

b. No

23. How far do you think financial institutions provide sufficient information and support regarding online security?

a. Highly agree

b. Agree

c. Neutral

d. Disagree

e. Highly disagree

24. how secure do you feel when conducting online banking transactions?

a. Very high

b. High

c. Neutral

d. Often

e. Less often

25. Based on your experiences, do you have specific recommendations for improving online banking security?

a. Yes

b. No

26. If your answer is no to the previous question, then state the reason.

Ans.