Open Banking System in Ireland: University Students' Perceptions on Data Security and Privacy

Submitted to:

Paul Walsh

Dublin Business school

Submitted By

Name: Quddus Ur Rehman Mumtaz

Student ID: 10626801

Declaration

I, Quddus Ur Rehman Mumtaz, hereby declare the research on the topic of ***"Open Banking System in Ireland: University Students' Perceptions on Data Security and Privacy"***. I have worked diligently and independently to complete this research on time. The dissertation was created by me; I state with utmost sincerity.

I also confirm that I followed all of the university's rules and regulations and didn't use any biased materials in my research. Furthermore, I certify that all necessary ethical considerations were taken during this research.

Name: ***Quddus Ur Rehman Mumtaz***

Date: 29th August, 2023

Place: Dublin Business school

Acknowledgement

I, Quddus Ur Rehman Mumtaz, would like to express heartfelt appreciation to my teachers and mentors who have guided me and helped me achieve objective of the topic ***"Open Banking System in Ireland: University Students' Perceptions on Data Security and Privacy"*** from the starting to the end. They've been helpful all along the research process. Without the support of my supervisor and the direction they gave me to complete the dissertation, the study would be significantly diminished.

The university's support has been invaluable as I've worked to complete my degree, I'm thankful for that. Finally, I'd like to express my gratitude to the people who, both before and after I finished the research, were there for me and showed their support.

Name: ***Quddus Ur Rehman Mumtaz***

Date: 29th August, 2023

Place: Dublin Business school

Abstract

Understanding user data security and privacy perceptions is crucial as open banking systems change and reshape the financial landscape. This study examines Irish university students' views on open banking. Students' security and privacy are examined through various relevant indicators confidentiality, integrity, availability, verification and. privacy This study analyses the complex relationship between three dimensions i.e. confidentiality, integrity, verification and user perceptions to illuminate the factors that affect open banking adoption and trust.A diverse sample of Irish university students was surveyed quantitatively using a quantitative research method through deductive approach. The aforementioned three dimensions' associations with students' security and privacy perceptions are significant. Students' increased concern for personal and financial privacy is evident in their confidentiality concerns. Data integrity also builds trust, as financial data accuracy and consistency are crucial. User perceptions are also improved by robust open banking verification mechanisms. User confidence in system security increases with efficient and effective verification processes. The study emphasizes user empowerment, transparent communication, and education in shaping open banking data security and privacy perceptions. The implications of these findings are vast. These insights will help financial institutions, technology providers, and policymakers create user-centric open banking systems that meet Irish university students' needs. By prioritizing confidentiality, data integrity, and verification, stakeholders can build trust, adoption, and open banking in Ireland. Therefore, this study fills a crucial gap in open banking user perceptions. The study allows academia and industry to improve data security, prioritize user trust, and shape open banking systems in a rapidly changing financial landscape.

Contents

Table of Figure

Chapter One: Introduction

1.1. Background of this study

The traditional banking system is transitioning towards open banking system that allows banks, within the legislative or regulatory requirements, to share customer information securely with third-party service providers, upon the customer's explicit consent, via standardized open application programming interfaces (APIs), enabling the delivery of valuable and innovative financial services that may involve data integration from various sources, as well as providing alternative payment initiation options (Nicholls, 2019). Its journey was started and facilitated in Europe by the European Union (EU) in 2015. Along EU, the European Parliament, the Euro Retail Payment Board (ERPB) and the berlin group promoted the ideas of open banking system, made and integrated directives, rules and regulations regarding the innovative online and mobile payment system in the European states (Berlin Group, 2020; European Commission, 2015; ERPB, 2019). In the United Kingdom (UK), several banks have developed novel digital business models (BMs) providing individuals and businesses with access to tailored financial services (Ramdani et al., 2020). Currently, the open banking system is being integrated in many countries as international financial organizations suggesting to adopt the system. For Ireland, International Monetary Fund (IMF) provided economic guidelines, suggesting the Irish government to continue its efforts to adopt instant payment system, and address the challenges hindering the adoption of open banking system in the country (IMF, 2020). In this regard, data security and privacy-related challenges can appear while the users of open banking system availing their financial service through sharing bank data with third parties. This issue is more focused in the European context, as the cyber security and privacy related issues are considered crucial. Arner et al. (2021) mentioned that strict data protection rules and regulations reflect European socio-cultural concerns

regarding dominant actors in the data processing field. The Bank of Ireland is considering these issues and publishing the information on the data security issues, and trying to convince people on this issue, as the good perceptions and trust of the citizens towards this new and innovative open banking systems, especially in data security and privacy issues, can contribute in the system's overall growth that can contribute in the Irish economy significantly. But there is lacking in primary research on the perceptions of the people regarding the issues of data security and privacy in the open banking system. This research is an attempt to address this gap.

1.2. Problem statement

The rise of open banking system led customers to explicitly authorize third-party firms to access their personal banking data for additional services, resulting in innovative financial products and tools, such as financial management platforms that consolidate multiple accounts, seamless interbank payment transmissions, small-value transactions, and mortgage comparison tools. Consequently, the financial services landscape, once vertically integrated by banks, is now being unbundled, with non-bank third parties, like fintech firms, offering services, and creating opportunities for banks to leverage and enhance the overall delivery chain—these collective phenomena constitute the essence of open banking (Report on Open Banking and Application Programming Interfaces (APIs), 2019). With the widespread adoption of open banking systems on a global scale, the paramount issue of data security and privacy is garnering significant attention, primarily driven by the perceived inadequacies in banks' cybersecurity capabilities (Zeller & Lynch, 2021). Kellezi et al. (2019) further highlight the potential for multiple cybersecurity challenges arising from the exposure of bank data to third-party providers without the implementation of robust security guidelines. This heightened concern underscores the urgency of addressing cybersecurity vulnerabilities in open banking environments to safeguard sensitive

customer information effectively. However, revised PSD2 guarantees the customers' data and privacy security, which is contributing in revolutionizing the relationship between banks and customers, creates opportunities for FinTech business models. But, a study reveals that, though the open banking system has a great market potential among young, active users of digital finance, it does not contribute in the improvement of financial inclusion for several reasons, including customers' preferences for anonymity and data sharing reluctance (Polasik & Kotkowski, 2022). In order to foster greater adoption of open banking systems among the younger generation, it is imperative to address their current perceptions concerning security issues, as data sharing reluctance results in deterring them from utilizing the open banking. To initiate this transformation, an essential first step involves conducting an in-depth assessment of their existing perceptions regarding open banking systems, as well as their concerns pertaining to data security and privacy protection. Understanding their perceptions on these crucial matters can offer valuable insights for financial policymakers, enabling them to design strategies that enhance young individuals' knowledge and awareness concerning data security and privacy in the context of open banking. This research is a scientific approach to understand the Irish University Students' perceptions of data security and privacy, and to identify the factors influencing their perceptions in the context of open banking system.

1.3. Objectives of the Study

1. To assess the Irish University Students' perceptions of data security and privacy in the context of open banking system.
2. To identify the factors that influence their perceptions regarding data security and privacy in the open banking system.

1.4. Research Question

1. What are the perceptions of University Students regarding data security and privacy in the open banking system in Ireland?

2. What are the factors that influence university students' perceptions regarding the open banking system's data security and privacy?

1.5. Structure of the Dissertation

Chapters	Contents Description
Introduction	The detailed background, strong study rationale, clear problem statement, relevant and specific research's goals and objectives.
Literature Review	Collecting books. Journals, paper and articles from credible sources. However, creating the literature gap is also done here.
Research Methodology	Process, methods, approaches, design, strategies and guidance for collecting more reliable facts to achieve research goals. Moreover Relevant ethical guidelines were followed when collecting facts.
Data Analysis/ Results	The facts that have been collected from credible sources have been effectively analyzed here.
Discussion	This section highlighted the key findings from analyzing the data supporting evidence which also improve research acceptability.
Conclusion and Recommendations	Analysing discussed aspects achieved all goals. Suitable recommendations for future endeavours can improve academic research success.

Chapter Two: Literature Review

2.1. Open Banking System

Open banking is a popular phenomenon in the banking sector (Briones De Araluze & Cassinello Plaza, 2022). Open banking gives customers more control over their financial data, boosts competition, and empowers them. APIs allow third-party developers to access and use client banking data with consent. Open banking is changing banking and financial services worldwide (Premchand & Choudhry, 2018).

UK, Australia, Canada, and other European countries have launched open banking policies. Each nation has its own regulations and execution methods. The UK's Open Banking Implementation Entity's 2016 Open Banking Standard required the nine largest banks to provide open APIs for authorised third-party providers (Almehrej et al., 2020). The 2018 Revised Payment Services Directive (PSD2) in the EU requires banks to share consumer data with licensed third-party suppliers (Steennot, 2018).

Open banking helps clients acquire personalized financial services like budgeting apps, financial counselling, and loan platforms by securely sharing their financial data with third-party suppliers (Babina et al., 2022). Open banking encourages banks and fintech startups to collaborate on new goods and services. Open banking increases financial sector competition, which improves price, customer service, and product offerings (Omarini, 2018).

Open banking's pros and cons have been studied. Open banking offers convenience, variety, and innovative services, but data security and privacy concerns have arisen (Remolina, 2019; Xiong et al., 2021). The system's openness raises concerns regarding customer financial data security and misuse. Open banking data security and privacy perspectives have been studied. It has been

examined that UK bank consumers about open banking and concluded that data security and privacy were their main concerns. Participants worried about data breaches, unauthorized access, and data control (Borgogno & Colangelo, 2020; Van Zeeland & Pierson, 2021).

Another study found that data security and privacy affected customers' trust in the Australian open banking ecosystem. To address customers' concerns and create trust in open banking services, the study stressed straightforward communication and explicit information sharing (Zeller & Dahdal, 2021). Susanto et al., (2013) examined how South Koreans trust open banking. The study found that data security and privacy protection influenced trust. The open banking system's reputation, security, and data protection standards increased trust. These studies emphasize the need of knowing open banking data security and privacy perceptions. These impressions affect customers' adoption and acceptance of open banking services; hence they must be examined. Policymakers, banks, and fintech startups can use these elements to improve open banking data security and privacy.

2.2. Privacy and Security in Open Banking System

In recent years, open banking, which gives third-party providers API access to customer banking data, has garnered interest. Open banking improves financial services and competitiveness, but data security and privacy are problems (Briones De Araluze & Cassinello Plaza, 2022).. Assessing open banking attitude requires understanding Irish university students' data security and privacy views. Studies on online financial transaction privacy and security can inform open banking. Govender & Sihlali (2014) did an extended study on university students' mobile banking security views. Mobile banking was seen as more secure and private by students than traditional banking. Unauthorized access, data breaches, and personal data misuse remained concerns. Irish university students may have similar open banking worries but that requires a separate study.

Online financial transactions raise privacy concerns. Van Zeeland & Pierson, (2021) examined consumer privacy problems in digital banking. Financial firms' data collecting and utilization worried participants. They were concerned about third parties accessing their personal data without their authorization. Third-party suppliers can access financial data in the open banking system, raising privacy issues. Open banking attitudes also depend on security. Nosrati & Bidgoli, (2016) explored mobile banking security concerns. The analysis found financial fraud, account hacking, and other security concerns. These worries show that people value financial data security and anticipate strong protections. Irish university students may share open banking security worries (Moscato & Altschuller, 2014).

Irish university students' views on open banking data security and privacy are likely to match those of prior studies. Security risks include money fraud and unauthorized account access, while privacy concerns include abuse of personal information (Shonola & Joy, 2014). Understanding these attitudes allows governments and financial organizations to address Irish university students' privacy and security concerns and ensure effective data protection in the open banking system. Addressing concerns and ensuring the effective deployment of the open banking system requires understanding the elements that affect people's views of data security and privacy.

Consumer trust greatly impacts online banking data security and privacy views. It has been examined that online financial service trust. Security, privacy, integrity, and confidentiality were found to increase confidence. These findings imply that Irish university students' perceptions of open banking data security and privacy may be influenced by their trust in websites and platforms (Al-Sharafi & Ruzaini, 2016). Security affects open banking data security and privacy perceptions. Özlen & Djedovic, (2017) examined online transaction privacy and security perceptions. Encryption, secure authentication, and data protection were stressed in the study. Strong security

measures can improve Irish university students' views on open banking data security and privacy (Aljawarneh, 2017; Maghrabi, 2014).

Privacy concerns influence online banking data security and privacy perceptions. (*Are Data Privacy Concerns Driving Consumer Behavior?*, n.d.; Balapour et al., 2020) examined online transaction characteristics that influence personal information disclosure. The study found that personal data misuse and unauthorized access greatly impact privacy views. Irish university students' opinions of data security and privacy in the open banking system may be influenced by their personal data worries. Data security and privacy perceptions also depend on the open banking system's trustworthiness. Integrity guarantees data integrity during transmission and storage. Kaur & Arora, (2020) explored how perceived integrity affects online banking trust and intention. Data integrity was demonstrated to increase trust in online banking services. Thus, protecting the open banking system can improve Irish university students' data security and privacy views.

In the open banking system, confidentiality—protecting sensitive financial data from unauthorized access—affects data security and privacy views. (Decaro & Saleh, 2003; Yousafzai et al., 2005) examined online banking trust and adoption. The study stressed the necessity of financial transaction confidentiality and secure data storage and transfer in developing confidence. Irish university students' data security and privacy perceptions depend on the open banking system's financial data confidentiality.

Consumer trust—including security, privacy, integrity, and confidentiality—significantly impacts views (Bomil Suh & Ingoo Han, 2003). Understanding these characteristics allows regulators and financial firms to improve open banking data security and privacy, address concerns, and develop confidence among Irish university students and other users. However, university students' views on data security and privacy in open banking and their influences are to be explored specialty in

the context of Ireland. This literature review addresses the gap in research on students' perceptions of open banking and the factors that influence their use of technology-based banking services.

As a large user base for technology-based services, university students' views on data security and privacy in open banking are vital (Akturan & Tezcan, 2012). While consumer opinions of internet banking and financial technologies have been studied, university student attitudes of open banking have not. Online banking perceptions have been studied in several research. Consumers' trust in mobile banking was strongly influenced by perceived security and privacy threats (Kim et al., 2009). This research explores consumer attitudes, but it doesn't address specifically university students' open banking concerns. University students' opinions of data security and privacy in open banking are understudied. This demographic group is a major user of technology-based financial services, therefore understanding their specific attitudes and concerns is vital.

2.3. Literature Gap

Limited research has been conducted on Irish university students' perceptions of data security and privacy in relation to the open banking system. There is a lack of comprehensive understanding regarding how these concepts are perceived by this specific demographic in the Irish context. The existing literature has not adequately addressed the perspectives of younger individuals, particularly university students, who may hold unique attitudes and concerns regarding technology, privacy, and financial services within the context of an open banking system. There is also a research gap in the literature on the impact of privacy concerns on the adoption of new financial technologies, such as open banking, particularly among university students who are known for being early adopters of technology. There also lacks a comprehensive understanding of how

university students evaluate the perceived benefits (convenience, efficiency) and risks (privacy breaches, data misuse) associated with open banking in the existing literature. Moreover, there is a lack of translating research findings into policy recommendations that address the concerns and needs of university students in Ireland in the context of open banking.

This research aims to fill the existing gaps in the academic literature and enhance the practical understanding of university students' perceptions of data security and privacy in the open banking system in Ireland.

Chapter Three: Conceptual Framework

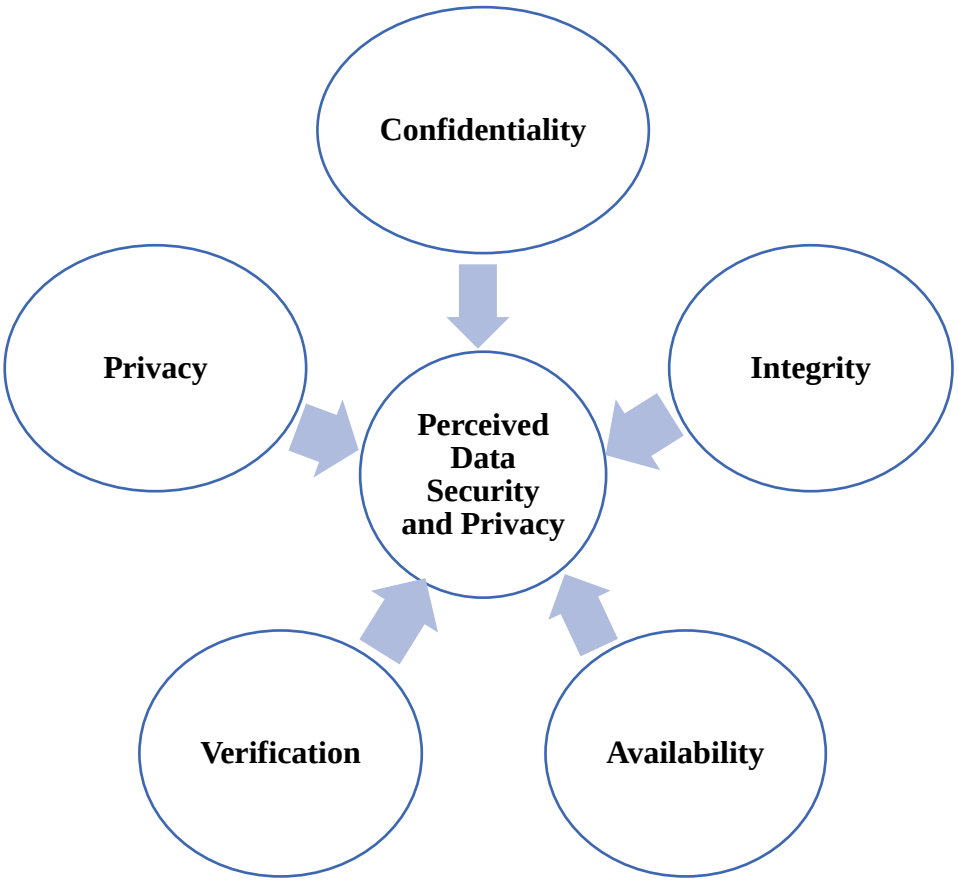


Figure 1: Conceptual Framework of the perceived data security and privacy

3.1. Independent variables

3.1.1. Confidentiality

Confidentiality refers to the act of preventing unauthorized disclosure of data to individuals or systems. Sarrafiaghdam (2003) emphasizes the significance of confidentiality in facilitating the secure transmission of data through identification. Confidentiality is a fundamental principle of data security and privacy (Parker, 2002) and plays a role in shaping customers' perception of information security. Sarrafiaghdam's (2003) study demonstrates that confidentiality strongly influences individuals' perception of security of data. The author argues that the alignment between

confidentiality and data security is crucial for instilling trust in the use of open banking systems. Encryption mechanisms are necessary to maintain the confidentiality of personal information and prevent unauthorized reading, copying, or disclosure (Ratnasingam, 2002).

3.1.2. Integrity

Integrity refers to the accuracy and assurance of transactions within a system application, ensuring that they have not been undetectably altered or deleted. Sarrafiaghdam (2003) revealed that integrity is a crucial component for ensuring the security of the open banking system. According to the CIA triad, the integrity of a data is compromised when it is intentionally altered during transmission. Data security systems commonly ensure both data confidentiality and data integrity. Customers depend on the integrity of open banking systems for conducting transactions. Web services employ reliable data to ensure data integrity and prevent duplication (Brodsky and Oakes, 2017).

3.1.3 Availability

Availability refers to the implementation of authorization mechanisms that ensure uninterrupted transmission and reception of transactions as required (Ratnasingam, 2002). To fulfill its intended function, an information system must ensure the timely availability of information. Computing systems utilized for information storage and processing necessitate robust security measures to safeguard against unauthorized access (Zeller and Dahdal, 2021). Availability maintenance includes measures to prevent denial of service attacks. Sarrafiaghdam (2003) highlights the significance of availability in data security and its impact on customer perception in open banking.

3.1.4. Verification

Verification ensures the authenticity of the domain name, providing evidence that customers are interacting with the legitimate open banking system (Almehrej, Freitas and Modesti, 2020). Verification is an essential aspect of every transaction conducted through open banking. It is imperative to implement customer verification, specifically through the utilization of a transaction authorization code (TAC) within the open banking application (Zeller and Lynch, 2020). The absence of implicit identity verification in electronic transactions allows for the creation of fraudulent websites. Customers may make errors when entering the domain name of Internet banks, such as typing "www.Citibank.net" instead of "www.Citibank.com" or misspelling "Citibank" as "Citybank" (Chellappa and Pavlou, 2001). Sullivan (2000) has documented numerous cases where websites have benefited from typographical errors.

3.1.5. Privacy

Privacy and data security have long been prominent topics in academic literature, extensively explored by numerous researchers. Smith et al. (1996) examined the relationship between privacy and risk and trust. Data collection, unauthorized access, inaccuracies, and secondary use were all scrutinized in detail as part of their research. The term "privacy" is used to describe the open banking system's ability to protect the privacy of individual customers' financial and identification data. Additionally, Sheng et al. (2008) emphasized the impact of privacy on customers' transaction behavior. Customers who use electronic financial services may have concerns about privacy due to the perceived ease with which their personal can be accessed by others on the internet (Jones et al., 2000). Customers are skeptical about the ability of privacy policies to maintain the confidentiality of their information (Gerrard and Cunningham, 2003).

3.2. Dependent Variable

Here, students' perceived data security and privacy is the dependent variable. For instance-

3.2.1. Perceived data security and privacy:

To investigate this dependent variable, the researchers have gathered data from university students using various methods such as surveys, and interviews. Thus, the data have been consisting of students' responses, opinions, and perceptions regarding their perceived level of data security and privacy when utilizing Open Banking systems in Ireland.

Hypotheses

H1: There exists relationship between Confidentiality and perceived data security and privacy in open banking system of Ireland.

H2: There exists relationship between Integrity and perceived data security and privacy in open banking system of Ireland.

H3: There exists a relationship between availability and perceived data security and privacy in open banking system of Ireland.

H4: Verification is related to the perception of data security and privacy in open banking system of Ireland.

H5: There exists relationship between Privacy and perceived data security and privacy in open banking system of Ireland.

Chapter Four: Methodology

This methodology chapter denotes the methods the study has used to answer the research questions through collecting external data and analyzing them using various methods, approaches, design,

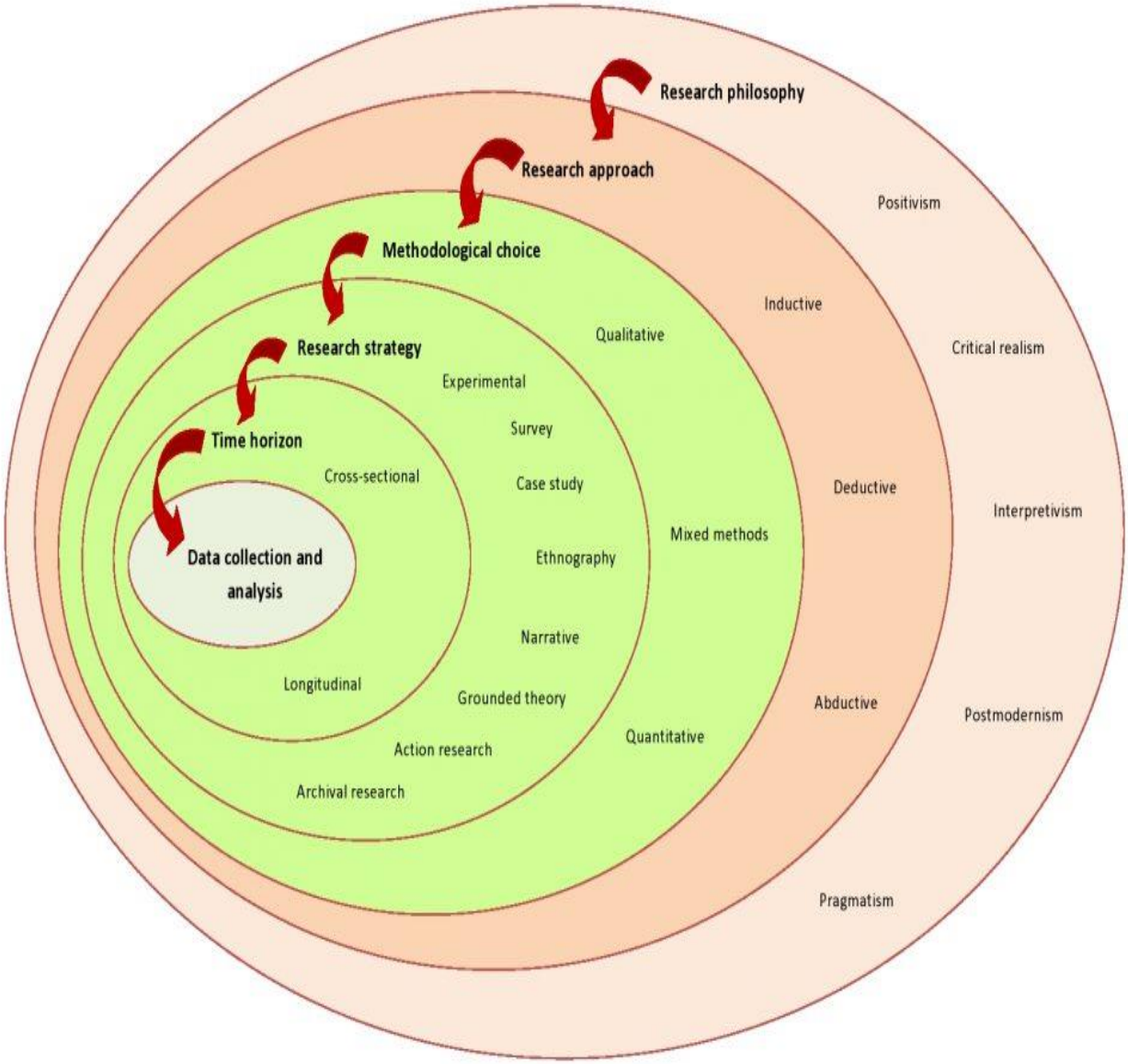


Figure 2: Saunder's Research Onion

data collection method, strategies, and analysis methods. This chapter followed Saunders' research onion for the study (Saunders, Lewis and Thornhill, 2019) (figure).

4.1. Research Philosophy

Research philosophies include pragmatism, interpretivism, and positivism. This study collected data on employee engagement and customers using **positivism**. Ryan (2018) claims that positivism research has focused on social facts that control society's members. This philosophy emphasizes structured methods like questionnaires to quantify observations. Quantified observations greatly aided positivism-based statistical analysis. This philosophy expressed the mechanisms operated by open banking system that greatly influence the students' perception about data security and privacy in open banking system of Ireland. Positivism helped analyzee quantified data, so it was used for quantitative study like this one (Turyahikayo, 2021).

4.2. Research Approach

This study used **deductive** logical approach. According to Svensson (2009), the deductive approach moves from general to specific. The study begins with a general observation and then draws specific conclusions. The deductive approach generated a hypothesis from the theory and observed students' perception and situation of data security and privacy indiactors (Casula, Rangarajan and Shields, 2020). The hypothesis observations helped collect and analyse data by testing to confirm their validity, including the ones needed for the study (Azungah, 2018). The study's hypothesis is rejected if validity fails. (Casula, Rangarajan, and Shields, 2020). Therefore, deductive approaches are considered in this research because they helped draw conclusions from specific observations.

4.3. Research Design

This study describes the population and situation using a **descriptive** research design. According to Sampetua Hariandja and Vincent (2022), the descriptive design of the study helps answer real-life questions with quantitative descriptions. This design provided a detailed description based on research questions to answer them. Descriptive research design helps answer this study's questions about students' perception engagement and open banking data security and privacy. Researching open banking mechanism in Ireland and irish students' perception regarding data security and privacy. However, Olubayo, Oloyede, and Lawal (2020) stated that the descriptive design greatly facilitates information gathering through questionnaires and observations. Thus, descriptive design was used to gather detailed information about the research questions to meet the study's goals.

4.4. Research Strategy

This study uses primary and secondary quantitative research methods. The primary quantitative study used a survey based on students' perception about data security and privacyin open banking system of Ireland. Apuke (2017) believes the primary quantitative research strategy is to collect data directly from survey participants without researching past data. This was followed by secondary quantitative research to complement the findings. Thus, this study used primary and secondary quantitative methods to gather data on employee students' perceived data security and privacy in open banking system of Ireland.

4.5. Methodological choice

Research choices include mono- and multi-method data collection. This study used multi-quantitative methods that were important. The multi-quantitative study uses primary and secondary quantitative methods to complete the study systematically. Greener (2018) suggests

collecting data using primary quantitative methods to gather a wide range of information. The information was collected from student who experience open banking services regularly. This study shows that various indicators like confidentiality, integrity and verification drives students' perception about open banking data security and privacy in ireland by linking primary and secondary quantitative choices (Zlatanović, 2017). Thus, the multi-quantitative approach has been successful in achieving the study's goals by gathering necessary data.

4.6. Research Time Horizon

Cross-sectional Research Design: This study provides a momentary snapshot of university students' perceptions of data security and privacy in Open Banking systems in Ireland. Researchers have analyzed the relationships between independent and dependent variables and made inferences about the perceptions of the population by collecting data from multiple students simultaneously, without the need to observe changes in perceptions over time.

4.6. Data Collection

Sampling

The students at the universities of Ireland using an open banking system are the population of the study. Non-probability sampling is used to select 59 participants for the study due to inadequate estimation of population numbers in the study context. Convenient sampling techniques have been used to reach those 59 respondents for the study from the population.

Choosing participants

Data was collected from the respondents through Google Forms containing the questionnaire was sent to the different students at different universities with their voluntary participation. Being university students The respondents are between 18 to 40 years old and Both male and female.

Quantitative Data Analysis

Quantitative data aimed to collect through Survey has been statistically examined. Closed-ended survey questions with numerical scales or predefined options would have provided quantitative data for the researchers. Participants rated data security and privacy statements from 1 to 5. After entering the data into spreadsheet software, SPSS has been employed to analyze it.

- **Descriptive Statistics:** Mean, median, mode, and standard deviation have been calculated to summarize and describe response distribution. These statistics illustrate participants' views on data security and privacy.
- **Frequency Analysis:** Frequency analysis determined how many participants chose each response option for specific questions. This analysis shows the most and least common responses.
- **Correlation Analysis:** The researchers examined variable relationships using correlation analysis. They compared data security and privacy perceptions to independent variables like confidentiality, integrity, availability, verification, and privacy.
- **Regression Analysis:** Regression analysis has assessed the strength and significance of relationships between multiple independent variables and students' perceived data security and privacy.
- **Data Visualization:** The findings have been visualized with bar charts, pie charts, histograms, or scatter plots.

4.3. Research Ethics

The research ethics has been thoroughly considered in this study. Such as- No respondent has been selected at the age of below 18 and above 70. Participants have been given informed consent and their privacy and confidentiality have been safeguarded. Participants have the freedom so they can leave the study at any moment without penalty. After being invited to participate and instructed on the study's purpose, the volunteer participants received a page of information about the study's goals, methods, limitations, and benefits. Participants have been informed that their participation is optional and that they can leave the study at any time without penalty. Participants have also been informed that their information would definitely be kept confidential. Participants have got unique identifiable codes to protect their privacy, and all the study data have been kept confidential. Only the researchers would have the access to the data, which have been anonymized. The questionnaire is non-invasive and does not hurt participants. There are no conflicts of interest. The study has been conducted with fairness and voluntary participation of the study respondents.

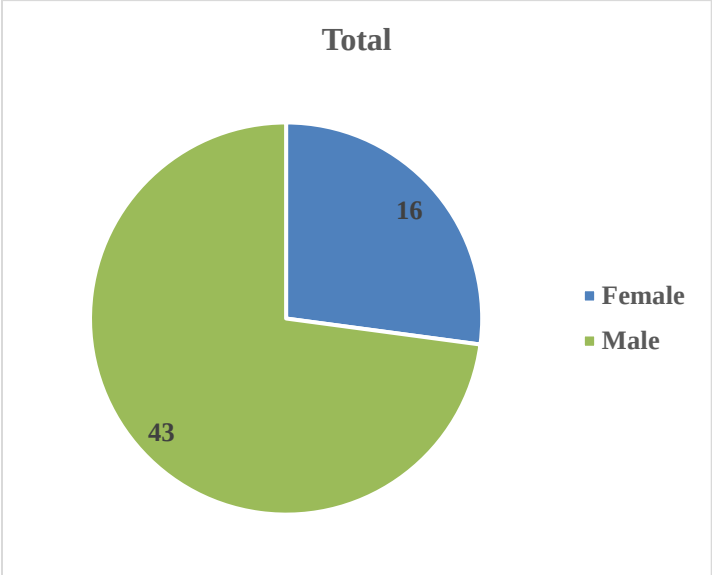
4.5. Limitations

- ***Sampling:*** Even though this study employed a common sampling method, the sample size was too small to draw meaningful conclusions. This study was limited to data from 59 participants due to time and material constraints. Any extrapolation of the results of this study is limited by the small size of the sample.
- ***Time and resource:*** Because of constraints on both resources and time, the researcher in this study had no leeway in how she went about her work. If the researcher had sufficient time and resources, they could dig deeper into the problem.

Chapter Four: Findings and Analysis

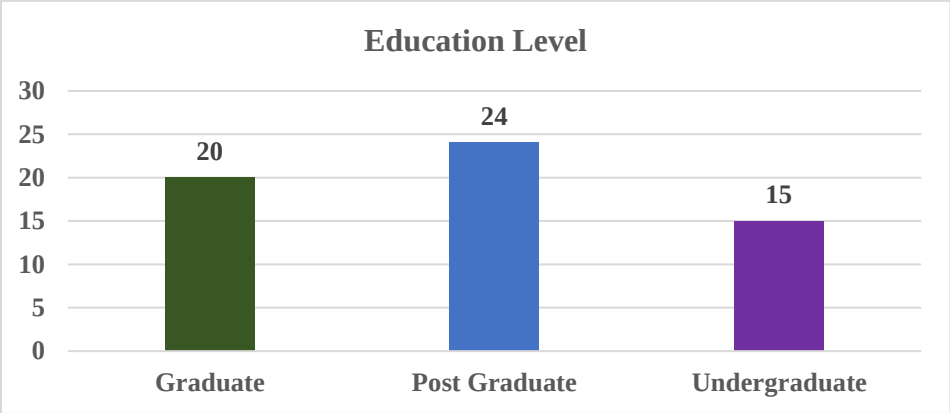
4.1. Demographic Information

- **Gender of the Respondents:**



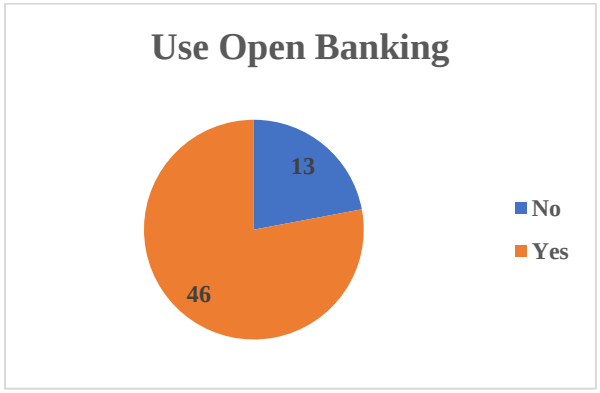
In this Research, the responses are taken from the students as it is a quantitative study of assessing the perception of students regarding the data security and privacy in th open banking system of Ireland. Here, the survey respondents were from both the male and female gender groups. Besides, it is seen that the male was more in number than the female as it is explicit that 43 respondents were male and the rest 16 respondents were female.

- **Education Level of the Respondents:**



The respondents were from different education level background. For instance, some were undergraduate, some were graduate, and the rest were post-graduate. In this study, 20 respondents were graduate, 24 respondents were post-graduate, and the rest 15 respondents were undergraduate level students. Hence, it is clearly observed that the respondents from the post graduate level are more in number and the undergraduate students are the less in number among all the respondents within this particular study.

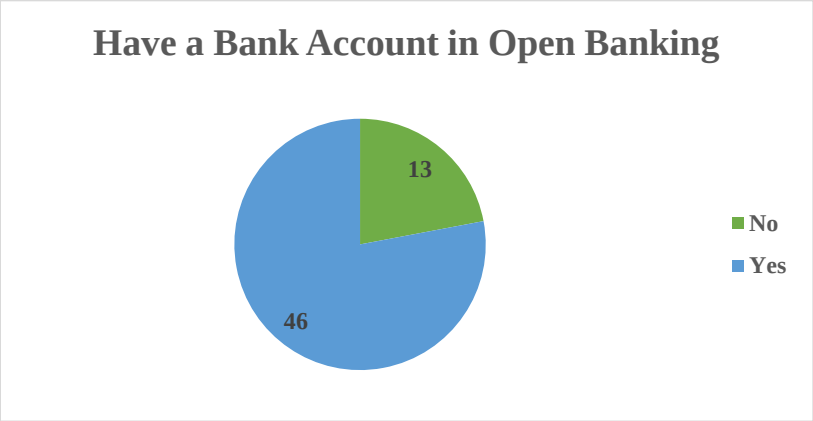
- **Status of Using Open Banking System:**



In this survey investigation, the participants are mostly the users of the Open Banking system of Ireland. Such as, 46 out of 59 respondents of this survey said that they are using open banking system of Ireland at this moment. On the other hand, the rest 13 respondents have stated that they

are not the users of the Open Banking system of Ireland. Hence, there are differences in the perception among the users and the non-users of the Open Banking System of Ireland.

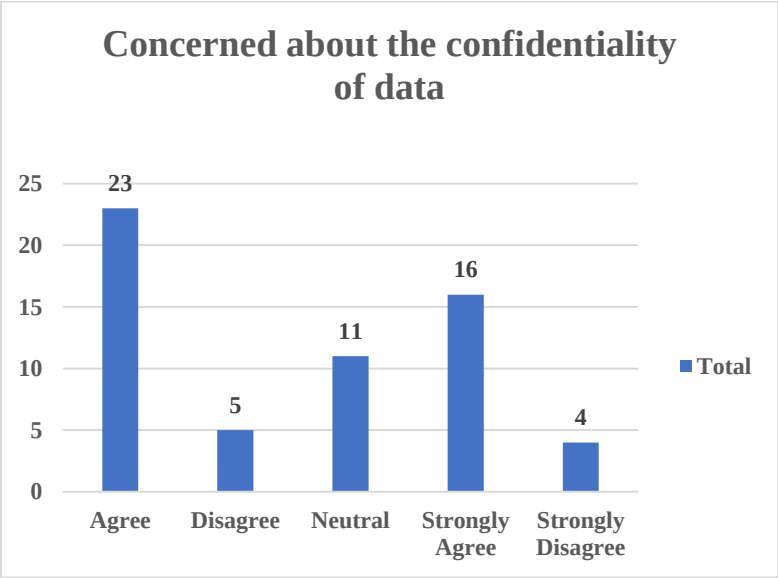
- **Having a bank account in open banking system:**



Among all the respondents, most of the respondents have said that they have bank accounts in the open banking system of Ireland. 46 respondents of this study have said that they have bank account in this open banking system. On the other hand, 13 respondents said that they don't have a bank account in the open banking system of Ireland. Thus, the perception of the students within this study are mostly based on the experience of their using and having a bank account in the open banking system of Ireland.

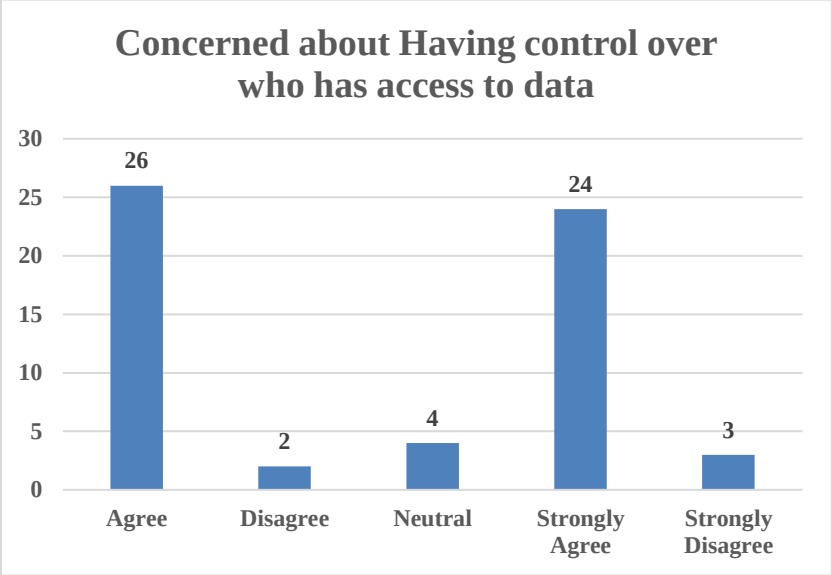
4.2. Confidentiality and Perceived Security and privacy in Open Banking System of Ireland

- **Concern about the confidentiality of my personal and financial data -**



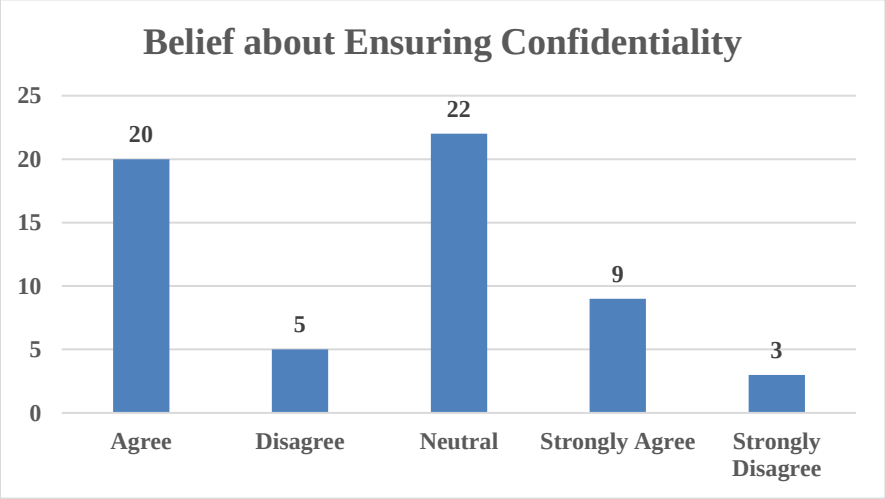
In this research, the respondents i.e. the students of Irish Universities were asked about whether they have been concerned about the confidentiality of their personal and financial data in the open banking system of Ireland. They have responded that are they mostly concerned about confidentiality of their financial and personal data within the open banking system. The result of the survey shows that 23 out of 59 respondents said that they agree the statement while additional 16 respondents strongly agreed with the statement that they are concerned about the financial and personal confidentiality of their data within the open banking system of Ireland. On the other hand, a total of 9 respondents out of 59 respondents disagreed with the statement. Which indicates that the 9 respondents are not concerned about the confidentiality of their personal and financial data in the open banking system of Ireland. Thus, it is clear that most of the students are concerned about the confidentiality of their personal and financial data in the open banking system of Ireland.

- **Concern about Having control over who has access to my personal and financial data-**



In this segment, the researcher has endeavored to assess whether it is important to the students to have control over who has access to my personal and financial data in the open banking system of Ireland. The survey outcomes demonstrate that most of the respondents have agreed with the statement. For instance, it has been found that a total of 50 respondents out of 59 have said that they feel it important to have control over who has access to my personal and financial data in the open banking system of Ireland. On the contrary, only 5 respondents have claimed that it is not important to them to have control over who has access to my personal and financial data in the open banking system of Ireland.

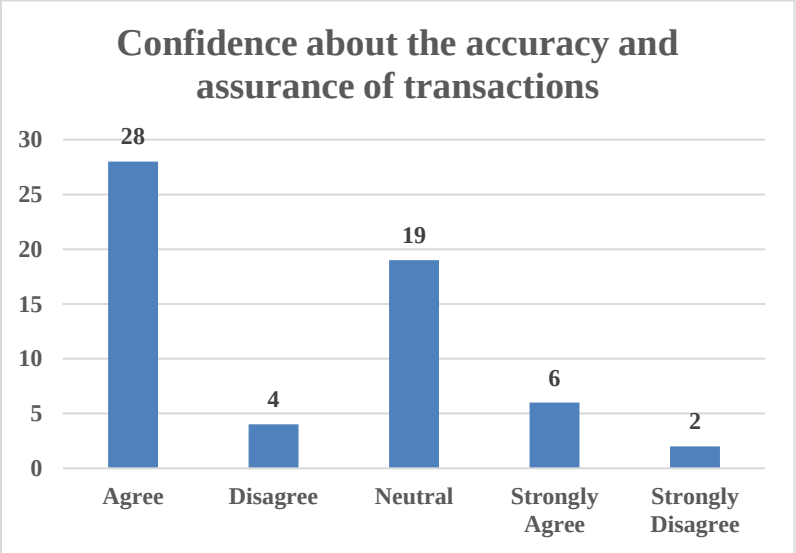
- **Belief about the open banking system's ensuring the confidentiality of data-**



In this study, the respondents were asked whether they have belief about the open banking system's ensuring the confidentiality of data. It has been found that most of the respondents have agreed with the statement although there is a significant portion of the students who doesn't have any positive or negative responses regarding this particular aspect. Which indicates that a remarkable segment of students is unaware of the fact of believing that open banking system in Ireland ensure the confidentiality of data. The data of this study demonstrate that a total of 29 respondents said they have belief that open banking system ensure the confidentiality of data. However, 22 respondents of this study are neutral and don't have any opinion. On the contrary, the rest 8 respondent have responded in negative and said that they don't have belief in the open banking system's ensuring the confidentiality of data.

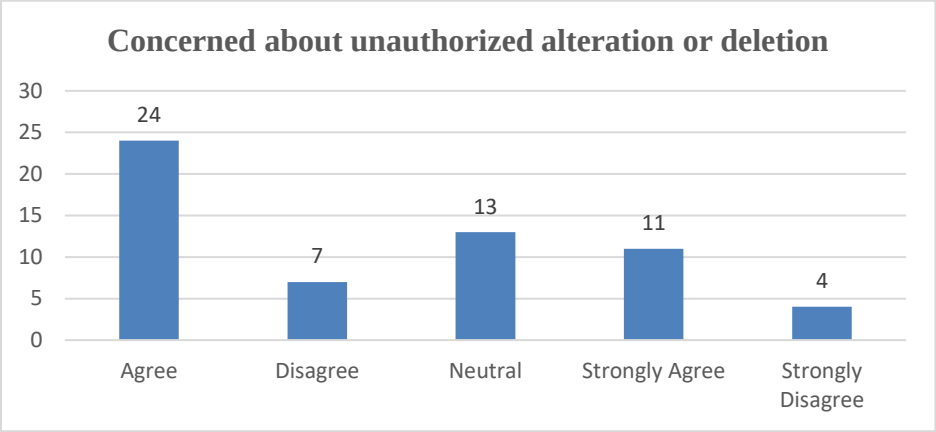
4.2. Integrity and Perceived Security and privacy in Open Banking System of Ireland

- **Confidence about the accuracy and assurance of transactions-**



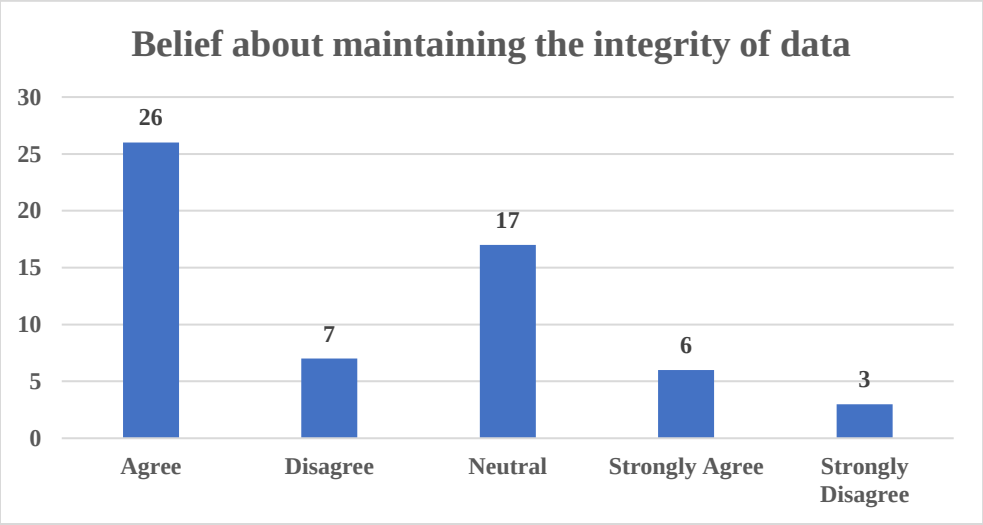
In this study, most of the students have claimed that they have confidence about the accuracy and assurance of transactions in the open banking system of Ireland. However, there are a great portion of the respondents have no positive or negative reaction. For example, 36 respondents out of the 59 respondents have claimed that they have Confidence about the accuracy and assurance of transactions within the open banking system of Ireland. Nevertheless, 19 respondents have not responded either positively or negatively. On the other hand, a total of 6 respondents have disagreed with the statement and indicated that they have no Confidence about the accuracy and assurance of transactions within the open banking system of Ireland.

- **Concern about unauthorized alteration or deletion of data -**



The survey respondents were asked regarding their concerns about unauthorized alteration or deletion of data within the open banking system of Ireland. In responses, most of the respondents have said that they were agreed that they have concern about unauthorized alteration or deletion of data although there are also individuals who are neutral in this case. Also, some respondents were seen to disagree with the statement. In this study, a total of 35 students have agreed with the statement that they have concern about unauthorized alteration or deletion of data. On the other hand, 11 students have claimed that they don't have any concern about unauthorized alteration or deletion of data. However, a significant portion i.e. 13 respondents were seen to stay neutral.

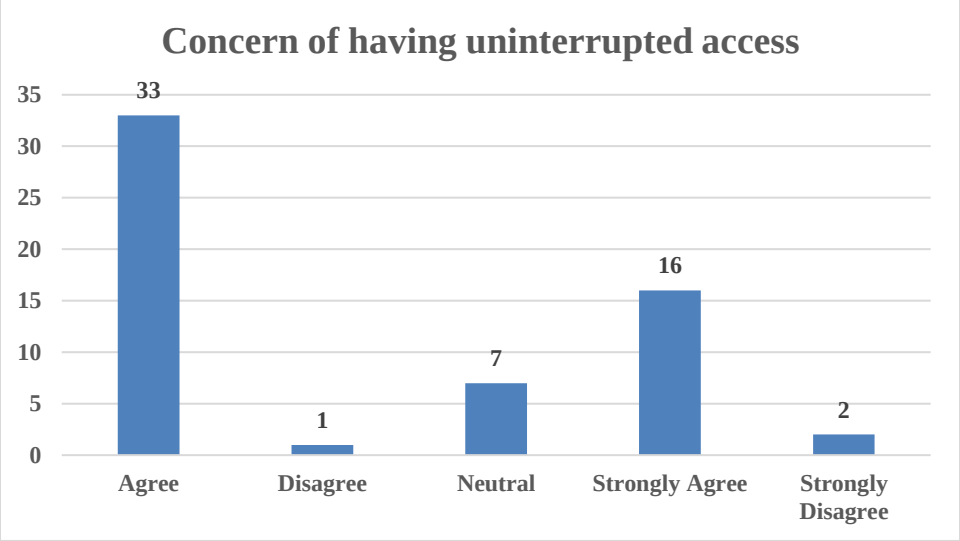
- **Belief about the open banking system's maintaining the integrity of data-**



While the respondents were asked about whether they have Belief about the open banking system's maintaining the integrity of data, most of the respondents i.e. a total of 32 out of 59 have agreed with the statement that they have belief in the open banking system's maintaining integrity. However, there is a significant number of respondents i.e. 17 students who were neutral in providing their responses. In the contrary, a total of 10 respondents have disagreed with the statement that they don't have belief in the open banking system's maintaining integrity within the context of Ireland.

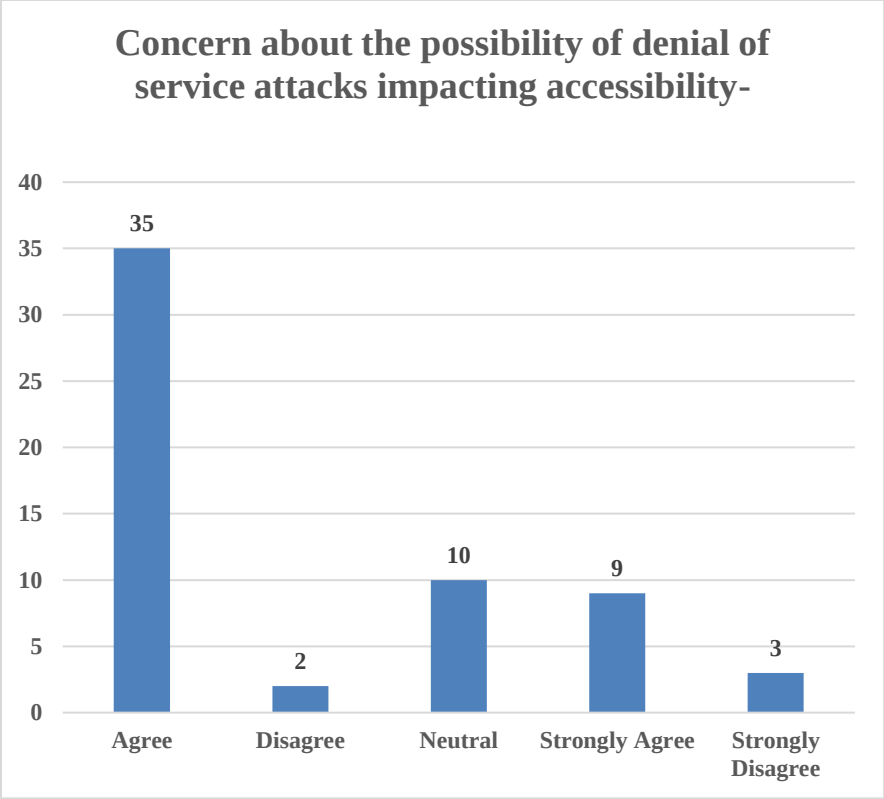
4.3. Availability and Perceived Security and privacy in Open Banking System of Ireland

- **Concern of having uninterrupted access to the open banking system-**



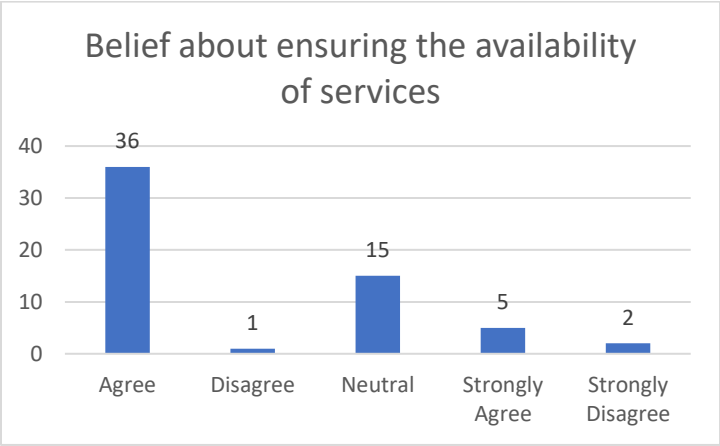
The survey respondents were asked regarding their concerns about unauthorized access to the open banking system of Ireland. In responses, most of the respondents have said that they were agreed that they have concern about unauthorized a access to the open banking system. Also, some respondents were seen to disagree with the statement. In this study, a total of 49 students have agreed with the statement that they have concern about unauthorized alteration or deletion of data. On the other hand, 3 students have claimed that they don't have any access to the open banking system of Ireland.

- **Concern about the possibility of denial of service attacks impacting accessibility-**



In this research, the respondents i.e. the students of Irish Universities were asked about whether they have been concerned about the possibility of denial of service attacks impacting accessibility of Ireland. They have responded that they are mostly concerned about concern about the possibility of denial of service attacks impacting accessibility of the students. The result of the survey shows that 35 out of 59 respondents said that they agree the statement while additional 9 respondents strongly agreed with the statement that they are concern about the possibility of denial of service attacks impacting accessibility of Ireland. On the other hand, a total of 5 respondents out of 59 respondents disagreed with the statement. Which indicates that the 5 respondents are not concerned about the concern about the possibility of denial of service attacks impacting accessibility within Ireland. Thus, it is clear that most of the students are concerned about the concern about the possibility of denial of service attacks impacting accessibility of Ireland.

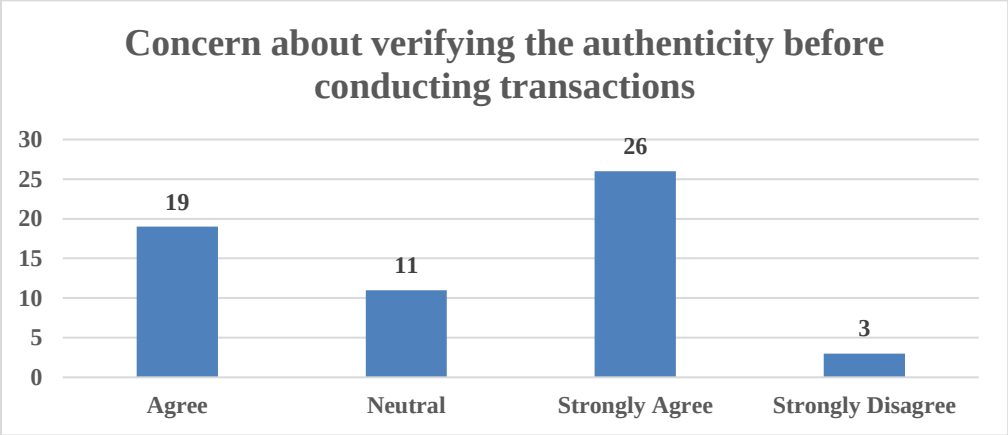
- **Belief about the open banking system's ensuring the availability of services-**



While the respondents were asked about whether they have Belief about the open banking system's ensuring the availability of services, most of the respondents i.e. a total of 41 out of 59 have agreed with the statement that they have belief in the open banking system's ensuring availability of services. However, there is a significant number of respondents i.e. 15 students who were neutral in providing their responses. In the contrary, a total of 6 respondents have disagreed with the statement that they don't have belief in the open banking system's ensuring availability of data within the context of Ireland.

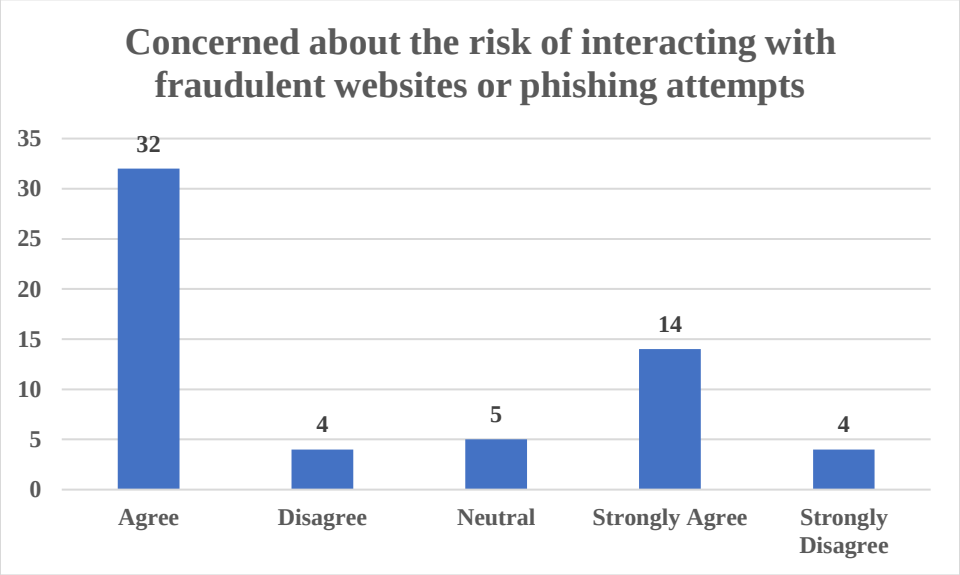
4.4. Verification and Perceived Security and privacy in Open Banking System of Ireland

- **Concern about verifying the authenticity of the open banking system before conducting transactions-**



The survey respondents were asked regarding their concerns about verifying the authenticity of the open banking system before conducting transactions within the open banking system of Ireland. In responses, most of the respondents have said that they were agreed that they have concern about verifying the authenticity of the open banking system before conducting transactions within the open banking system. Also, some respondents were seen to disagree with the statement. In this study, a total of 45 students have agreed with the statement that they have concern about. On the other hand, 3 students have claimed that they don't have any concern relate to the open banking system of Ireland.

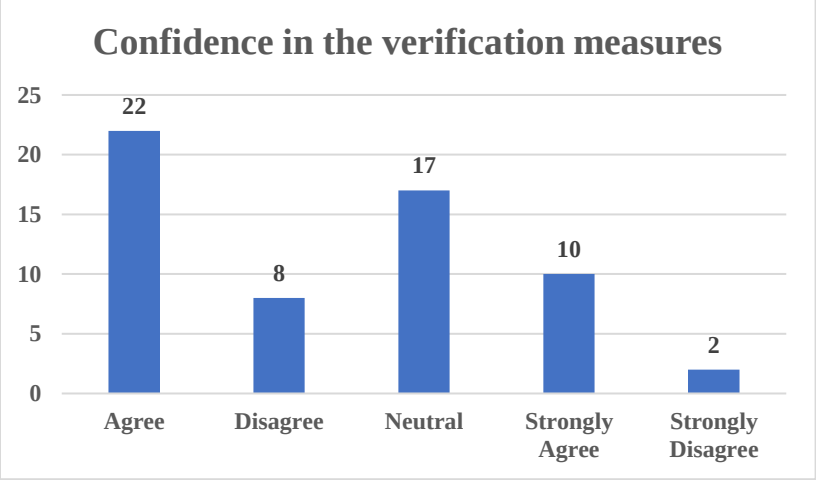
- **Concern about the risk of interacting with fraudulent websites or phishing attempts in the open banking system-**



In this research, the respondents i.e. the students of Irish Universities were asked about whether they have been Concern about risk of interacting with fraudulent websites or phishing attempts in the open banking system of Ireland. They have responded that are they mostly have concerns about the risk of interacting with fraudulent websites or phishing attempts in the open banking system. The result of the survey shows that 32 out of 59 respondents said that they agree the statement while additional 14 respondents strongly agreed with the statement that they are concerned about risk of interacting with fraudulent websites or phishing attempts in the open banking system of Ireland. On the other hand, a total of 9 respondents out of 59 respondents disagreed with the statement. Which indicates that the 9 respondents are not concerned about risk of interacting with

fraudulent websites or phishing attempts in the open banking system of Ireland. Thus, it is clear that most of the students are concerned about the risk of interacting with fraudulent websites or phishing attempts in the open banking system of Ireland.

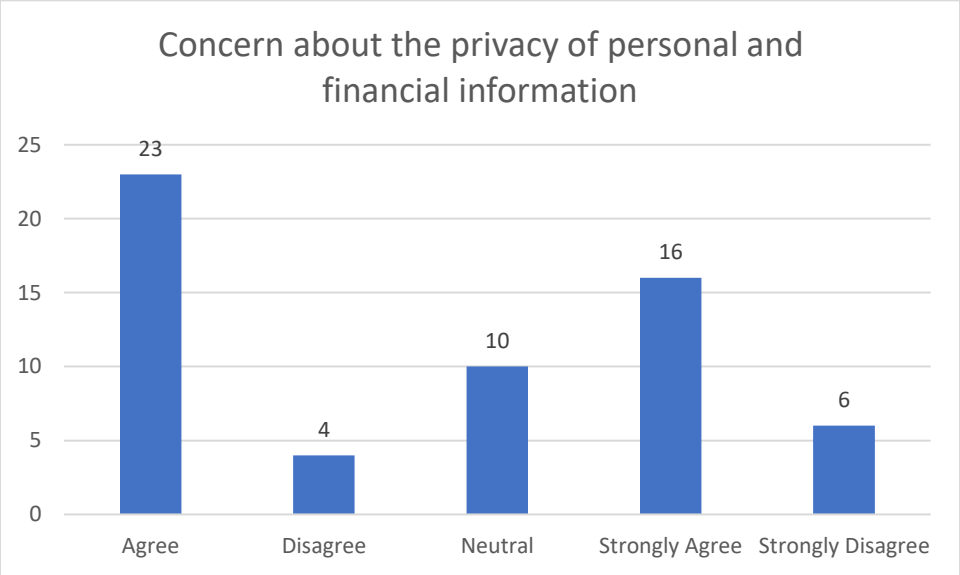
- **Confidence in the verification measures implemented by the open banking system-**



In this study, most of the students have claimed that they have confidence in the verification measures implemented by the open banking system open banking system of Ireland. However, there are a great portion of the respondents have no positive or negative reaction. For example, a total 32 respondents out of the 59 respondents have claimed that they have Confidence about the verification within the open banking system of Ireland. Nevertheless, 17 respondents have not responded either positively or negatively. On the other hand, a total of 10 respondents have disagreed with the statement and indicated that they have no Confidence in the verification measures implemented by the open banking system of Ireland.

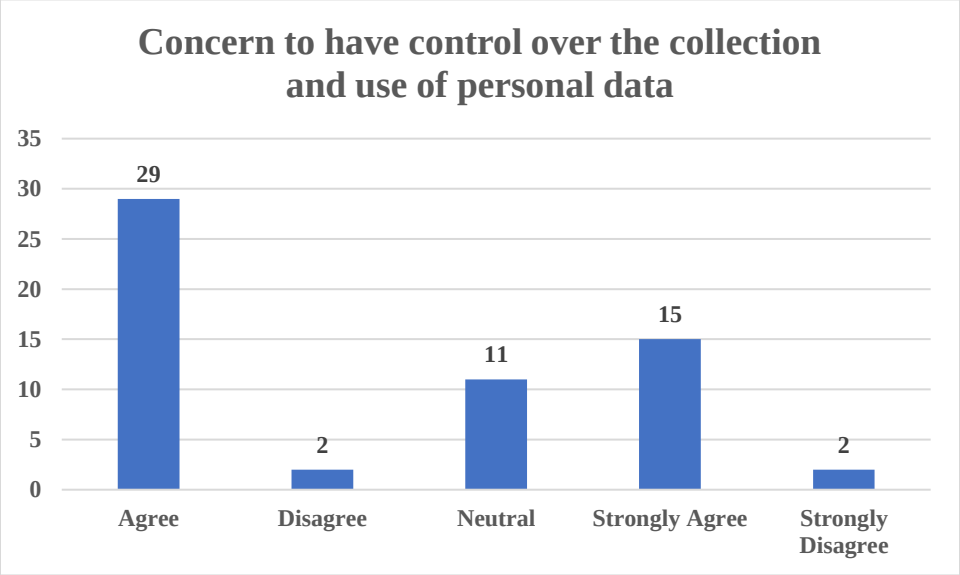
4.5. privacy and Perceived Security and privacy in Open Banking System of ireland

- **Concern about the privacy of personal and financial information in the open banking system-**



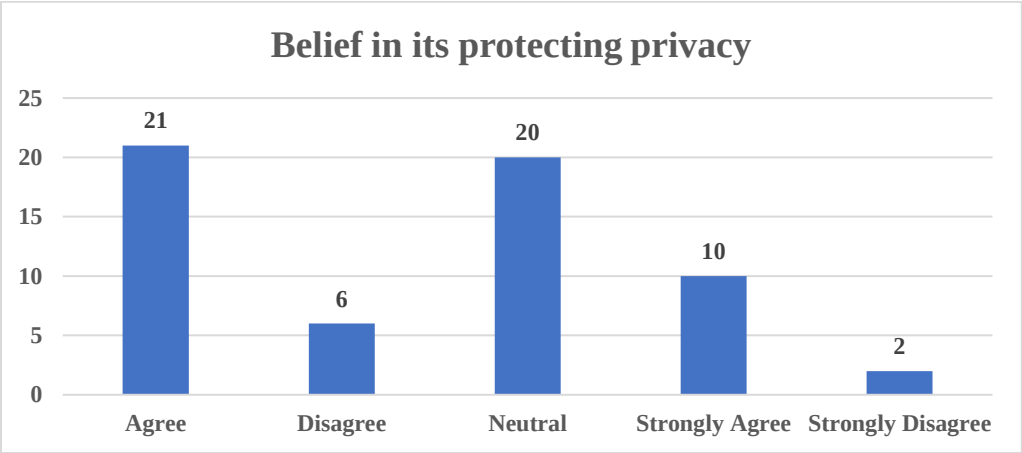
In this research, the respondents i.e. the students of Irish Universities were asked about whether they have been Concern about the privacy of personal and financial information in the open banking system of Ireland. They have responded that are they mostly Concern about the privacy of personal and financial information in the open banking system. The result of the survey shows that 23 out of 59 respondents said that they agree the statement while additional 16 respondents strongly agreed with the statement that they are concerned about the financial and personal privacy of their data within the open banking system of Ireland. On the other hand, a total of 9 respondents out of 59 respondents disagreed with the statement. Which indicates that the 10 respondents are not concerned about the privacy of their personal and financial data in the open banking system of Ireland. Thus, it is clear that most of the students are concerned about the confidentiality of their personal and financial data in the open banking system of Ireland.

- **Concern to have control over the collection and use of personal data in the open banking system-**



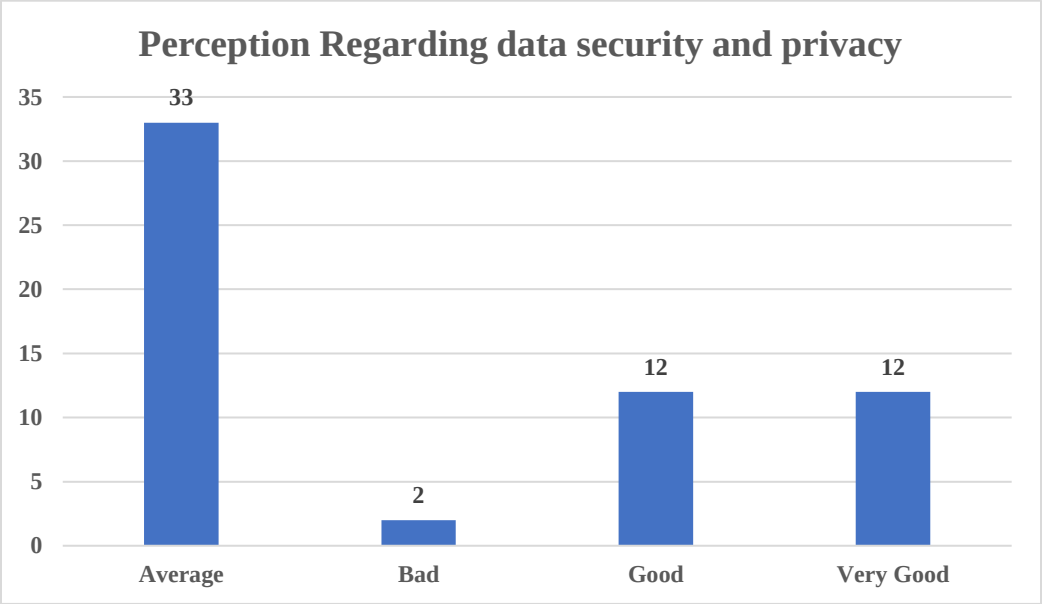
The researcher has endeavored to assess whether it is important to the students to have control over the collection and use of personal data in the open banking system of Ireland. The survey outcomes demonstrate that most of the respondents have agreed with the statement. For instance, it has been found that a total of 44 respondents out of 59 have said that they feel it important to have control over the collection and use of personal data in the open banking system of Ireland. On the contrary, only 4 respondents have claimed that it is not important to them to have control over the collection and use of personal data in the open banking system of Ireland. In the meantime, 11 persons were neutral in providing responses.

- **Belief in the open banking system's protecting privacy-**



While the respondents were asked about whether they have belief in the open banking system's protecting privacy, most of the respondents i.e. a total of 31 out of 59 have agreed with the statement that they have belief in the open banking system's protecting privacy. However, there is a significant number of respondents i.e. 20 students who were neutral in providing their responses. In the contrary, a total of 8 respondents have disagreed with the statement that they don't have belief in the open banking system's protecting privacy within the context of Ireland.

4.6. Perception Regarding data security and privacy in the open banking system -



Most of the respondents of this study have stated that they have an average perception regarding the data security and privacy in the open banking system. The survey result shows that 33 respondents out of the 59 respondents have claimed that their perception regarding data security and privacy in the open banking system of Ireland is average. Meanwhile, a total of 24 individual have said that they have a good perception about the data security and privacy in the open banking system of Ireland. However, 2 respondents have argued that their perception about data security and privacy in the open banking system is bad.

4.6. Correlation Analysis

According to Jahangir and Begum (2008), Pearson correlation is used to examine the relationship betweenthe variables. If the value of correlation coefficient ranges from 0.10 to 0.29 is considered weak. Meanwhile the value range from 0.30 to 0.49 is considered medium and from 0.50 to 1.0 is considered strong, according to Wong and Hiew (2005). There is also an indicator that the correlation coefficient should not go beyond 0.8 to avoid multi-collinearity (Field, 2005). Multi-collinearity occurs when two or more variables in the model are correlated and provide redundant information. It is often confusing and lead to misleading results. As indicated in the following table, correlation coefficient is less than 0.8, therefore it is assumed that multi collinearity problem existsin this research

Correlation					
	CF	IF	AF	VF	PF
CF	1	.445**	.294*	.500**	.321*
IF	.445**	1	.273*	0.241	.360**
AF	.294*	.273*	1	.549**	.331*
VF	.500**	0.241	.549**	1	.596**
PF	.321*	.360**	.331*	.596**	1
**. Correlation is significant at the 0.01 level (2-tailed).					
*. Correlation is significant at the 0.05 level (2-tailed).					

There are strong relationships between all the variables as the respective correlation is above 0.5. Furthermore, the sig (2-tailed) values are less than 0.05 indicated that there are statistically

significant correlations between variables. Therefore, if any of the variable increases or decreases, the other variables also increase or decreases

4.7. Regression Analysis

Regression analysis is a constructive statistical technique that can be used to analyze the associations between a set of independent variables and a single dependent variable (Hair et al., 2005). Multiple regressions are used to examine the relationship between perceived information security, integrity, availability, verification and privacy.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.517[a]	.267	.198	.766

a. Predictors: (Constant), Privacy, Confidentiality, Integrity, Availability, Verification

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.326	5	2.265	3.863	.005[b]
	Residual	31.080	53	.586		

	Total	42.407	58			

a. Dependent Variable: I perceive data security and privacy in the open banking system as-

b. Predictors: (Constant), Privacy, Confidentiality, Integrity, Availability, Verification

Based on table 6, it can be observed that the R Square was 0.267, representing that 26.7 percent of the perceived data security and privacy can be explained by privacy, integrity, availability, confidentiality and verification. It can be concluded the following equation:

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.964	.467		4.210	.000
	Confidentiality	-.357	.147	-.433	-2.430	.019
	Integrity	.494	.159	.535	3.100	.003
	Availability	-.318	.187	-.324	-1.703	.094
	Verification	.552	.171	.693	3.236	.002
	Privacy	-.163	.159	-.198	-1.023	.311

a. Dependent Variable: Perceived data security and privacy in the open banking system.

Perceived Information Security = β1 Confidentiality + β2 Integrity + β3 Availability + β4 Verification + β5 Privacy + ε

Perceived Information Security = -.357* Confidentiality + 0.494 * Integrity – 0.318 * Availability + 0.552* Verification - 0.163* Privacy + 1.946

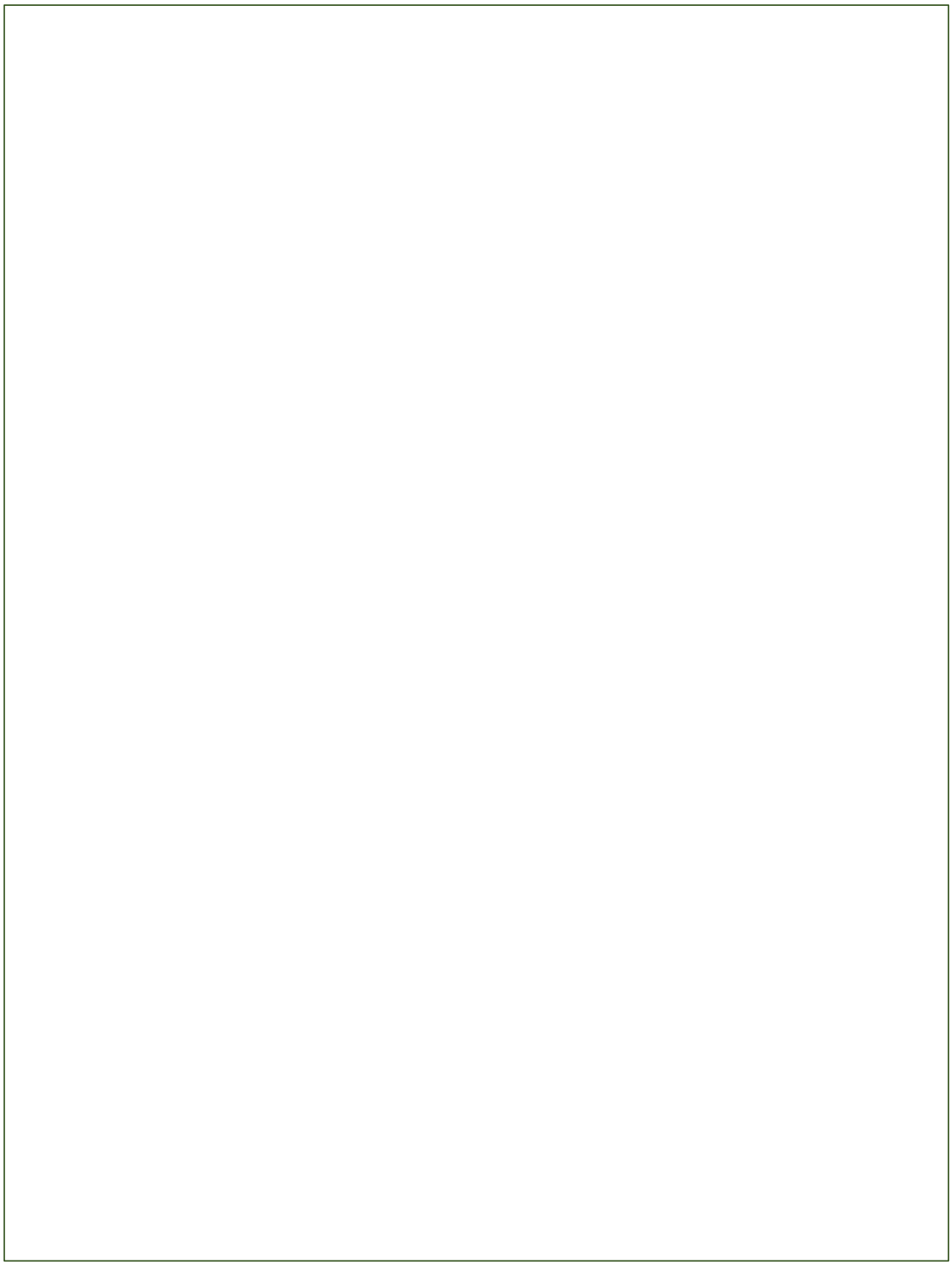
For the individual variables reveals that confidentially (t-value = -2.430 and $p<0.05$), integrity (t-value= 3.100 and $p<0.05$) and Verification (t-value= 3.236 and $p<0.05$) were found to have a significant relationship with perceived information security.

Therefore, the hypotheses H1, H2 and H4 were supported. Meanwhile Availability (t-value = -1.703 and $p>0.05$) and Privacy (t-value = -1.023and $p>0.05$) had no significant

relationship with the perceived information security. Hence, H3 and H5 are not supported.

4.8. Hypothesis Test Outcome

Hyppotheses	Accepted?	Rejected
H1: There exists relationship between Confidentiality and perceived data security and privacy in open banking system of Ireland.	Yes	No
H2: There exists relationship between Integrity and perceived data security and privacy in open banking system of Ireland.	Yes	No
H3: There exists a relationship between availability and perceived data security and privacy in open banking system of Ireland.	No	Yes
H4: Verification is related to the perception of data security and privacy in open banking system of Ireland.	Yes	No
H5: There exists relationship between Privacy and perceived data security and privacy in open banking system of Ireland.	No	Yes



Chapter Five: Discussion

This section evaluates the findings of this study regarding the interrelationships among indicators of perceived data security and privacy (confidentiality, authentication, authorization, non-repudiation, privacy) and their association on students' perception towards data security and privacy in open banking system of Ireland. The analysis conducted in the previous chapter confirms a positive correlation between perceived security and data in the open banking system of Ireland. This study aimed to examine Irish university students' perceptions of data security and privacy in the open banking system. The study demonstrates significant correlations between the perceptions of students and three important dimensions: confidentiality, integrity, and verification. The following discussion situates these findings within the current body of literature, emphasizing their significance for both academic and industrial sectors.

5.1. Confidentiality and perceptions of data security

Our findings support previous research that highlights the importance of confidentiality in influencing perceptions of data security and privacy (Dinev & Hart, 2006; Krasnova et al., 2010). University students are highly concerned about safeguarding their personal and financial data. Confidentiality is crucial in the open banking system, as it highlights the need for strong encryption, secure data transmission, and data compartmentalization.

Data security relies on confidentiality to prevent unauthorized access, disclosure, and dissemination. In open banking, where financial transactions and personal data are shared electronically, user data confidentiality is crucial to trust and engagement. The study found a strong association between confidentiality and Irish university students' views on open banking data

security. The research shows that Irish university students are very sensitive to financial data privacy. These factors include the inherently private nature of financial information, the potential consequences of unauthorised access (such as identity theft or fraud), and the growing awareness of data breaches in the digital age. The research suggests that open banking system confidentiality measures are crucial to positive user perceptions. End-to-end encryption and SSL protocols protect data during transmission and storage. Data compartmentalization, which separates sensitive data layers, strengthens confidentiality. These measures protect user data from unauthorized parties. The findings also suggest that users, including university students, trust and are more confident when they have granular data sharing preferences. Users who can choose which data is shared, with whom, and why on open banking platforms empower them and protect their data. Transparent communication about how user data is handled, stored, and accessed boosts data security and confidentiality.

Thus, confidentiality underpins user perceptions of data security in open banking. Stakeholders can build trust and encourage Irish university students and the public to use open banking services by prioritising and improving data security.

5.2. Integrity and perceived security and privacy of open banking.

The correlation between integrity and students' perceptions highlights the importance of data integrity in building trust in the open banking industry. Trust plays a vital role in the acceptance of financial technologies by users (Siau & Wang, 2004). The open banking system's capacity to uphold the precision and uniformity of financial data is essential in establishing this trust. Maintaining data accuracy, minimizing errors, and preventing unauthorized modifications are

crucial for maintaining users' trust. Data integrity—its trustworthiness and accuracy throughout its lifecycle—is essential to data security. In open banking, where financial transactions and sensitive information are exchanged electronically, data integrity is essential for user trust and security and privacy. Irish university students' perceptions of open banking's security and privacy are strongly correlated with integrity.

Irish university students are more aware and sensitive to financial data integrity, according to the research. Data tampering in open banking can cause financial and reputational harm. These risks emphasize the importance of data integrity in user trust. Students' data security and privacy perceptions depend on their confidence in the system's financial data accuracy and consistency. Effective data integrity measures shape open banking user perceptions of security and privacy. Checksums, digital signatures, and hashing algorithms prevent data tampering. Real-time monitoring and anomaly detection help identify and address integrity breaches quickly. Open banking providers build user trust by ensuring information accuracy and reliability. The research suggests that integrity measures affect open banking user experience. Users who have consistent, error-free interactions trust the system and transact confidently. However, data discrepancies and errors can damage trust and raise security and privacy concerns. Creating a seamless and trustworthy user experience requires maintaining financial data integrity in the open banking system of Ireland.

5.3. Verification and perceived security and privacy of open banking.

Verification and user confidence are important factors to consider in various domains, such as online platforms and digital services. Verification, the third dimension, showed a significant association with students' perceptions. This highlights the significance of implementing strong user verification methods in open banking systems. Effective verification methods not only prevent

unauthorised access but also bolster user confidence in the system's security. The results support previous research that highlights the importance of multi-factor authentication in enhancing perceptions of security (Cao et al., 2019). Verification is a crucial part of data security that verifies the identity of users or entities accessing sensitive data or transacting. In open banking, where financial transactions are conducted electronically, robust verification mechanisms boost user confidence, ensure secure interactions, and shape security and privacy perceptions. Irish university students' perceptions of open banking's security and privacy are strongly correlated with verification.

The research emphasises the importance of verification in open banking trust. Users, especially Irish university students, prioritise identity verification and party verification. The open banking system's ability to verify users' and entities' identities builds trust. Students' data security and privacy perceptions depend on their trust in legitimate and authorised entities.The research suggests that strong verification mechanisms reduce the risk of unauthorised access. Multi-factor authentication (MFA), biometric verification, and other advanced methods protect accounts and sensitive data in open banking systems. Open banking providers improve user security and privacy by strengthening these measures to reduce data breaches and unauthorised transactions. The verification processes improve user experience by providing a sense of security. Efficient and effective verification mechanisms reassure users that their open banking interactions are safe. The assurance that their identity is protected from fraud improves their perception of the system's security and privacy.

5.4. The implications for academia and industry

These findings have significant implications for both the academic and industrial sectors. The study contributes to the existing literature by identifying key dimensions that have a significant impact on university students' perceptions. This highlights the complex nature of data security and privacy concerns in open banking, emphasizing the need to go beyond a simplistic approach in order to gain a deeper understanding of the factors that influence user attitudes. Moreover, the findings provide guidance for industry practitioners in designing open banking systems that address the concerns of university students. Robust confidentiality measures, data integrity assurance, and effective verification mechanisms are crucial for promoting positive perceptions and increasing adoption rates. Additionally, the research emphasizes the importance of clear and open communication regarding these measures in order to establish trust among users.

5.5. Limitations of the study and areas for future research.

Although this study offers valuable insights, it is not exempt from limitations. The sample consists mainly of university students, potentially reducing the generalizability of the findings to wider populations. Furthermore, this study primarily examines individuals' perceptions, which may not accurately correspond to their actual behaviours. Future research could employ a longitudinal methodology to examine the temporal evolution of perceptions and their translation into tangible decision-making outcomes.

Therefore, this research highlights the notable connections between confidentiality, integrity, verification, and the perceptions of Irish university students regarding data security and privacy in the open banking system. By considering these aspects, academia and industry can work together to establish a secure and user-friendly open banking ecosystem that meets the needs and expectations of the younger demographic.

Please be aware that this template is a general guide and should be customised to align with the specific findings and intricacies of your research project. In addition, it is important to include proper citations to reference the previously mentioned research studies.

Chapter Six: Conclusion and Recommendations

6.1. Conclusion

This research has delved into the perceptions of Irish university students concerning data security and privacy within the dynamic landscape of the open banking system. Through a systematic investigation of the research objectives and consideration of the independent variables, several significant insights have emerged. From the extensive research, it has been found that, among the five predetermined hypothesis, three hypotheses are proved significantly associated with the perception of the Irish university students towards the data security and privacy in open banking system in Ireland. Such as: Confidentiality, Integrity, and verification.

Here, the assessment of Irish university students' perceptions revealed a spectrum of attitudes towards data security and privacy within the context of open banking. While the students demonstrated a heightened concern regarding the confidentiality, integrity, and verification of their personal and financial information, considering of the risks associated with the open banking system. Furthermore, this study identified the key factors influencing the students' perceptions of data security and privacy. The variables of confidentiality, integrity, and verification played pivotal roles in shaping these perceptions. The robustness of data encryption methods, the extent of information control, and the reliability of authentication processes have directly impacted students' feelings of trust and security in utilizing open banking services. Furthermore, the findings of correlation analysis have underlined the interconnectedness of these factors. For instance, strong data integrity measures were found to bolster students' confidence not only in the security of their information but also in the overall privacy of their transactions.

6.2. Recommendations

Based on the research project's findings, which identified significant associations between Irish university students' perception and the concepts of confidentiality, integrity, and verification in the open banking system, the following recommendations are proposed:

1. Education and Awareness Enhancement: -

i) Implement educational initiatives and workshops specifically designed for university students to enhance their comprehension of data security and privacy within the framework of open banking.

ii) Establish partnerships with universities and financial institutions to integrate modules on data security, privacy, and open banking into applicable academic courses or workshops.

2. Communication and Transparency Enhancement: -

i) Financial institutions and open banking service providers should prioritize effective and transparent communication regarding their data security measures, privacy policies, and verification processes.

ii) Providing regular updates to university students and other users regarding any modifications or improvements implemented in the security infrastructure.

3. Emphasizing User-Centric Design: -

i) Developing open banking platforms and applications with a user-centric orientation, emphasising intuitive interfaces that empower users to exercise greater control over their data sharing and privacy preferences.'

ii) Developing user-friendly mechanisms to verify transactions and access sensitive information.

4. *Implementing Multi-Factor Authentication (MFA):*

i) As a standard security measure, MFA requires users to provide multiple forms of verification in order to access accounts or perform transactions.

ii) Informing the advantages of multi-factor authentication (MFA) and provide them with guidance on the proper setup and effective utilization of MFA.

5. *Enhancing User Control: -*

i) Enable users, including university students, to have precise control over the specific categories of data they choose to disclose to open banking services.

ii) Users should have the ability to easily withdraw access to their data and be provided with options to restrict data sharing to specific purposes.

6. *Addressing privacy concerns:-*

i) financial institutions and policymakers should work together to create and deploy privacy-enhancing technologies. These technologies should safeguard user data while ensuring smooth open banking experiences.

ii) Regularly perform audits and assessments of data handling practises to identify and address potential privacy vulnerabilities.

7. *Continuous monitoring and improvement:-*

i) implementing to identify security breaches, unauthorized access, or anomalies in the open banking system.

ii) Implementing a feedback mechanism to solicit input from university students regarding security measures, facilitating necessary enhancements.

Therefore, by implementing these recommendations, stakeholders will be able to collaborate in order to establish a safer and more secure open banking environment for Irish university students and users in general. The emphasis on confidentiality, integrity, and verification addresses the concerns and perceptions identified, thereby bridging the gap between user expectations and the practices in the open banking system.

Reference

Akturan, U., & Tezcan, N. (2012). Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence & Planning*, *30*(4), 444–459. https://doi.org/10.1108/02634501211231928.

Aljawarneh, S. A. (Ed.). (2017). *Online Banking Security Measures and Data Protection:* IGI Global. https://doi.org/10.4018/978-1-5225-0864-9.

Almehrej, A., Freitas, L. and Modesti, P., 2020. Account and Transaction Protocol of the Open Banking Standard. In *Rigorous State-Based Methods: 7th International Conference, ABZ 2020, Ulm, Germany, May 27–29, 2020, Proceedings 7* (pp. 230-236). Springer International Publishing.

Almehrej, A., Freitas, L., & Modesti, P. (2020). Account and Transaction Protocol of the Open Banking Standard. In A. Raschke, D. Méry, & F. Houdek (Eds.), *Rigorous State-Based Methods* (Vol. 12071, pp. 230–236). Springer International Publishing. https://doi.org/10.1007/978-3-030-48077-6_16.

Al-Sharafi, M. A., & Ruzaini, A. A. (2016). *The Impact of Customer Trust and Perception of Security and Privacy on the Acceptance of Online Banking Services: Structural Equation Modeling Approach*. https://www.semanticscholar.org/paper/The-Impact-of-Customer-Trust-and-Perception-of-and-Al-Sharafi-Ruzaini/aadbd1f32ac77b484a884d360c5cf63ce562e7e8.

Are data privacy concerns driving consumer behavior? Not yet. (n.d.). Deloitte Insights. Retrieved May 3, 2023, from https://www2.deloitte.com/us/en/insights/industry/technology/protecting-consumer-data.html

Arner, D. W., Buckley, R. P., & Zetzsche, D. A. (2021). *Open Banking, Open Data and Open Finance: Lessons from the European Union*. https://papers.ssrn.com/abstract=3961235

Babina, T., Buchak, G., & Gornall, W. (2022). Customer Data Access and Fintech Entry: Early Evidence from Open Banking. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4071214.

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Berlin Group starts new open Finance API Framework. (2020). The Berlin Group. https://www.berlin-group.org/single-post/press-release-berlin-group-starts-new-openfinance-api-framework

Bomil Suh & Ingoo Han. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce*, *7*(3), 135–161. https://doi.org/10.1080/10864415.2003.11044270.

Borgogno, O., & Colangelo, G. (2020). Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3513514.

Briones De Araluze, G. K., & Cassinello Plaza, N. (2022). Open banking: A bibliometric analysis-driven definition. *PLOS ONE*, *17*(10), e0275496. https://doi.org/10.1371/journal.pone.0275496.

Brodsky, L. and Oakes, L., 2017. Data sharing and open banking. *McKinsey & Company*, *1105*.

Chellappa, R.K. and P.A. Pavlou, 2002. "Perceived information security, financial liability and consumer trust in electronic commerce transactions", Logistics information Management, 15(5/6): 358-368.

Decaro, F., & Saleh, Z. I. (2003). *An examination of the internet security and its impact on trust and adoption of online banking*. https://www.semanticscholar.org/paper/An-examination-of-the-internet-security-and-its-on-Decaro-Saleh/5df3cfb860d3ebabdc0e47989557683ff2de511a

European Parliament adopts European Commission proposal to create safer and more innovative European payments. (2015). European Commission. https://ec.europa.eu/commission/presscorner/home/en

Gerrard, P. and J. Cunningham, 2003. "The diffusion of internet banking among Singapore consumers", International Journal of Bank Marketing, 21(1): 16-28

Govender, I., & Sihlali, W. (2014). A Study of Mobile Banking Adoption among University Students Using an Extended TAM. *Mediterranean Journal of Social Sciences*. https://doi.org/10.5901/mjss.2014.v5n7p451

Hutchinson, D. and M. Warren, 2001. "A framework of security authentication for internet banking", paper presented at the Conference on Information Integration and Web-based Applications & Services (IIWAS), September, Austrian Computer Society, Linz.

Ireland: Financial Sector Assessment Program-Technical Note on Oversight of Fintech (Country Report No. 22/243). (2022). IMF. https://www.imf.org/en/Publications/CR/Issues/2022/07/25/Ireland-Financial-Sector-Assessment-Program-Technical-Note-on-Oversight-of-Fintech-521281

Jones, S., M. Wilikens, P. Morris, M. Masera, 2000. "Trust requirements in e-business: a conceptual framework for understanding the needs and concerns of different stakeholders", Communications of the ACM, 43(12): 81-7.

Kaur, S., & 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), 1–30. https://doi.org/10.1108/JABS-08-2019-0252

Kellezi, D., Boegelund, C., & Meng, W. (2019). Towards Secure Open Banking Architecture: An Evaluation with OWASP. In J. K. Liu & X. Huang (Eds.), *Network and System Security* (Vol. 11928, pp. 185–198). Springer International Publishing. https://doi.org/10.1007/978-3-030-36938-5_11.

Kim, G., Shin, B., & Lee, H. G. (2009). Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, *19*(3), 283–311. https://doi.org/10.1111/j.1365-2575.2007.00269.x.

Maghrabi, L. A. (2014). The threats of data security over the Cloud as perceived by experts and university students. *2014 World Symposium on Computer Applications & Research (WSCAR)*, 1–6. https://doi.org/10.1109/WSCAR.2014.6916842.

Moscato, D. R., & Altschuller, S. (2014). International Perceptions of Online Banking Security Concerns. *Communications of the IIMA*, *12*(3). https://doi.org/10.58729/1941-6687.1193

Nosrati, L., & Bidgoli, A. M. (2016). A review of mobile banking security. *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–5. https://doi.org/10.1109/CCECE.2016.7726820.

Omarini, A. E. (2018). Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future. *International Business Research*, *11*(9), 23. https://doi.org/10.5539/ibr.v11n9p23.

Open Banking and the Rise of FinTech: Innovative - ProQuest. (n.d.). Retrieved July 31, 2023, from https://www.proquest.com/docview/2322611475?fromopenview=true&pq-origsite=gscholar

Özlen, M. K., & Djedovic, I. (2017). Online banking acceptance: The influence of perceived system security on perceived system quality. *Journal of Accounting and Management Information Systems*, *16*(1), 164–178. https://doi.org/10.24818/jamis.2017.01008

Parker, D.B., 2002. "Monitoring the workforce to support security objectives: a long-term view", RedSiren Technologies, Inc. (October).

Polasik, M., & Kotkowski, R. (2022). *The Open Banking Adoption Among Consumers in Europe: The Role of Privacy, Trust, and Digital Financial Inclusion* (SSRN Scholarly Paper No. 4105648). https://doi.org/10.2139/ssrn.4105648.

Premchand, A., & Choudhry, A. (2018). Open Banking & APIs for Transformation in Banking. *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 25–29. https://doi.org/10.1109/IC3IoT.2018.8668107.

Ramdani, B., Rothwell, B., & Boukrami, E. (2020). Open Banking: The Emergence of New Digital Business Models. *International Journal of Innovation and Technology Management*, *17*(05), 2050033. https://doi.org/10.1142/S0219877020500339.

Ratnasingam, P. and P. Pavlou, 2002. "Technology Trust: The Next Value Creator in B2B Electronic Commerce", International Resources Management Association Conference, Washington, Seattle.

Remolina, N. (2019). Open Banking: Regulatory challenges for a new form of financial intermediation in a data-driven world. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3475019.

Report of the ERPB Working Group on a Single Euro Payments Area (SEPA) Application Programming Interface (API) Access Scheme. (2019). Euro Retail Payment Board (ERPB). https://www.ecb.europa.eu/paym/groups/erpb/shared/pdf/11th-ERPB-meeting/Report_from_the_ERPB_WG_on_a_SEPA_API_Access_Scheme.pdf?18ac5087de445faeb7ca11f951bb7ca11f951bb7ca11f951bb7ca.

Report on open banking and application programming interfaces (APIs). (2019). BIS (Bank of International Settlements). https://www.bis.org/bcbs/publ/d486.htm

Sarratiagham, A., 2008. "Perceived information security and consumer trust in electronic commerce transactions: a survey of internet banking adoption in Malaysia,".

Sheng, H., F.F.H. Nah and K. Siau, 2008. "An experimental study on ubiquitous commerce adoption: impact of personalization and privacy corcerns," Journal of the AIS, 9(6): 344-76.

Shonola, S. A., & Joy, M. S. (2014). Mobile learning security concerns from university students' perspectives. *2014 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL2014)*, 165–172. https://doi.org/10.1109/IMCTL.2014.7011125

Smith, H.J., S.J. Milberg and S.J. Burke, 1996. "Information privacy : measuring individuals' concerns about organizational practices," MIS Quarterly, 20(2): 167-96.

Steennot, R. (2018). Reduced payer's liability for unauthorized payment transactions under the second Payment Services Directive (PSD2). *Computer Law & Security Review*, *34*(4), 954–964. https://doi.org/10.1016/j.clsr.2018.05.008.

Sullivan, B., 2000. "Making money off 'typosquatting': firms tap domain typos to grab clicks and ad bucks", in MSNBC Technology Section, 22 September, available at: http://zdnet.com.

Susanto, A., Lee, H., Zo, H., & Ciganek, A. P. (2013). Factors Affecting Internet Banking Success: A Comparative Investigation between Indonesia and South Korea. *Journal of Global Information Management*, *21*(2), 72–95. https://doi.org/10.4018/jgim.2013040104.

Van Zeeland, I., & Pierson, J. (2021). In Banks We Trust: Banks as Custodians of Personal Data in Open Banking Ecosystems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3896405.

Xiong, J., Hsiang, E.-L., He, Z., Zhan, T., & Wu, S.-T. (2021). Augmented reality and virtual reality displays: Emerging technologies and future perspectives. *Light: Science & Applications*, *10*(1), 216. https://doi.org/10.1038/s41377-021-00658-8.

Yousafzai, S. Y., Pallister, John. G., & Foxall, G. R. (2005). Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology & Marketing*, *22*(2), 181–201. https://doi.org/10.1002/mar.20054.

Zeller, B. and Dahdal, A.M., 2021. Open banking and open data in Australia: global context, innovation and consumer protection. *Qatar University College of Law, Working Paper Series, Working Paper*, (2021/001).

Zeller, B. and Lynch, B., 2020. Challenges in open banking-what are the practical steps to be taken now? *UW Austl. L. Rev.*, *48*, p.579.

Zeller, B., & Dahdal, A. M. (2021). Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3766076.

Zeller, B., & Lynch, B. (2021). Challenges in open banking - what are the practical steps to be taken now? *UNIVERSITY OF WESTERN AUSTRALIA LAW REVIEW*, *48*(2), 579–605. https://doi.org/10.3316/informit.20211206057900.

Appendices

<u>Research Project Title:</u> Open Banking System in Ireland: University Students' Perceptions on Data Security and Privacy

Consent Letter

Dear Respondent,

Greetings!

I would like to invite you to participate in a survey as part of an academic research titled "Open Banking System in Ireland: University Students' Perceptions on Data Security and Privacy". The purpose of this research is to assess University Students' Perceptions on Data Security and Privacy in the open Banking System of Ireland. Your valuable input will contribute to a better understanding of the issue.

Participation in this survey is completely voluntary, and your responses will be treated with strict confidentiality. No personal identifying information will be collected, and the data obtained will be used for research purposes only. Your participation will greatly contribute to the credibility and reliability of the research findings.

Request for completing the survey: Please read each question carefully and select the most appropriate response based on your personal experiences and opinions. By participating in this survey, you consent to the use of the collected data for research purposes.

Your time and contribution to this study are highly appreciated. Thank you for your willingness to participate and help advance the field of Business Studies.

Survey Questionnaire (Google-form)

Demographic Information

Age*

Your answer

Gender*

- Male
- Female
- Other

Educational Level *

- Undergraduate
- Graduate
- Post Graduate

Do you use Open Banking System? *

- Yes
- No

Do you have a bank account in open banking system? *

- Yes
- No

Confidentiality

I'm concerned about the confidentiality of my personal and financial data in the open banking system-*

Strongly disagree

- Disagree
- Neutral
- Agree
- Strongly Agree

It’s important for me to have control over who has access to my personal and financial data in the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I believe that the open banking system ensures the confidentiality of my data-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Integrity

I'm confident about the accuracy and assurance of transactions in the open banking system?*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I'm concerned about unauthorized alteration or deletion of my data in the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I believe that the open banking system maintains the integrity of my data-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Availability

It's important for me to have uninterrupted access to the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I'm concerned about the possibility of denial of service attacks impacting my access to the open banking system? *

- Strongly Disagree
- Disagree
- Neutral

- Agree
- Strongly Agree

I believe that the open banking system ensures the availability of its services-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Verification

It's important for me to verify the authenticity of the open banking system before conducting transactions? *

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I'm concerned about the risk of interacting with fraudulent websites or phishing attempts in the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I feel confident in the verification measures implemented by the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Privacy

I'm concerned about the privacy of my personal and financial information in the open banking system? *

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

It's important for me to have control over the collection and use of my personal data in the open banking system-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

I believe that the open banking system protects my privacy-*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Perceived data security and privacy

I perceive data security and privacy in the open banking system as-*

- Very Bad
- Bad
- Average
- Good
- Very Good

Thank You So Much for Your Kind Cooperation!