Iosr Journal Of Economics And Finance (Iosr-Jef)
E-Issn: 2321-5933, P-Issn: 2321-5925.Volume 16, Issue 2 Ser. 4 (Mar. – Apr. 2025), Pp 10-33
www.Iosrjournals.Org

Securing Online Payments: Understanding Cyber Threats And Safeguarding Financial Transactions

Ms. Accamma CG, Bhavya Kothari, Shibin, Akash V, Angana
Research Scholar, Assistant Professor, Jain - Center For Management Studies UG Student Jain - Center For Management Studies

Abstract
We live in a world where everything is connected—our phones, homes, cars, even the watches we wear. While this digital convenience makes life easier, it also opens the door to a growing and often invisible danger: cyber threats.
From stolen passwords to massive data leaks, cyberattacks have become a daily reality. Whether it's a small business being hit with ransomware or someone unknowingly falling for a phishing scam, the impact can be deeply personal and financially devastating. These threats aren't just coming from lone hackers anymore—many are part of organized groups or even backed by governments, making them more advanced and harder to stop.
As technology keeps evolving, so do the risks. Take smart safety wearables, for example. They're designed to protect us—tracking health, sending emergency alerts—but if not properly secured, they can be turned against us. A hacker could track someone's location or access sensitive health data, all without the user even knowing. This is just one of many examples of how vulnerable our digital lives can be.
The problem is, security often takes a backseat to convenience. Many people aren't aware of the risks, and companies don't always invest enough in protecting user data. As a result, cyber threats continue to grow—targeting schools, hospitals, banks, and even entire governments.
So what can we do? It's not just about using strong passwords anymore. We need smarter systems, better laws, regular updates, and more education on how to stay safe online. Cybersecurity isn't just a tech issue—it's a human issue. The more we understand the risks and take steps to protect ourselves and others, the safer our digital world will be.

Keywords: *Cyber threats, data breaches, ransomware, phishing, IoT security, smart devices, cybersecurity awareness, digital safety, human impact, tech vulnerabilities, online privacy.*

Date of Submission: 05-04-2025 Date of Acceptance: 15-04-2025

Chapter 1: Introduction to cyber security

The protection of computer systems and networks against malicious actors that could result in unauthorized information exposure, theft, or damage to hardware, software, or data, as well as in the disruption or misdirection of the services they provide, is known as technology security, cyber security, digital security, or information security (IT security).
The increased reliance on computers, the internet, and wireless network standards like Bluetooth and Wi-Fi makes the field important.

Also, because of the proliferation of smart bias, which includes multicolored bias that makes up the Internet of goods(IOT), cellphones, and boxes. Because of the complexity of information systems and the society they support, cyber security is one of the biggest problems facing the ultramodern world.

similar to power distribution, decision- timber, and finance, security is pivotal for systems that oversee expansive physical products.

What is cyber-security?

Cyber security refers to any technology, measure, or practice for precluding cyber-attacks or mollifying their impact. Cyber security aims to cover individualities' and associations' systems, operations, calculating bias, sensitive data and fiscal means against computer contagions, sophisticated and expensive rescue earthenware attacks, and more.

Cyber-attacks have the power to disrupt, damage, or destroy businesses, and the cost to victims keeps rising.
There are numerous common orders into which cyber security can be categorized.

Protecting a computer network from intrusions, such as opportunistic malware or targeted bushwhackers, is known as network security.
The goal of Z operation security is to prevent bias and software from becoming compromised. The data it is intended to cover could be accessed through a compromised operation. Effective security starts long before a program or device is deployed, during the design phase.

§ Information security protects the integrity and sequestration of data, both in storehouse and in conveyance.

functional security includes the processes and opinions for handling and guarding data means. The warrants druggies have when penetrating a network and the procedures that determine how and where data may be stored or participated all fall under this marquee. Disaster recovery and business durability define how an association responds to a cybersecurity incident or any other event that causes the loss of operations or data. Disaster recovery programs mandate how the association restores its operations and information to return to the same operating capacity as before the event. Business durability is the plan the association falls back on while trying to operate without certain coffers.

End- stoner education addresses the most changeable cyber-security factor people. Anyone can accidentally introduce a contagion to an otherwise secure system by failing to follow good security practices. tutoring druggies to cancel suspicious dispatch attachments, not plug in unidentified USB drives, and colorful other important assignments is vital for the security of any association.

IBM (International Business Machines) estimates that the price of a DATA BREACH 2023 report is

1. $ In 2023, the average cost of a data breach was USD 4.45 million, which is more than $150 million over the previous three years.
2. In 2023, the average cost of a data breach connected to rescue earthenware was also high, at USD million. This figure excludes the cost of the rescue payment, which was $890 more than it was previously and a superfluous USD.

Many times, the growing trends in information technology (IT) include: B an increase in the abandonment of personal computers, network complexity, remote work, and work from home

ll these trends produce tremendous business advantages and mortal progress but also give exponentially more for cybercriminals to attack.

A recent study set up that the global cyber security worker gap — the gap between being cyber security workers and cyber security jobs that need to be filled was 3.4 million workers worldwide.

2 Resource-strained security brigades are fastening on developing comprehensive cyber security strategies that use advanced analytics, artificial intelligence, and robotization to fight cyber pitfalls more effectively and minimize the impact of cyber-attacks.,

1. Overview of online payments:

A range of online payment methods is available, including digital wallets, wire transfers, debit and credit cards, as well as net banking. Customers can utilize these options to make online payments for subscriptions, mobile devices, DTH recharges, clothing, and various products from e-commerce platforms.

The online payment process encompasses four key participants: the customer, the merchant, the customer's bank, and the merchant's bank. Despite the involvement of multiple parties, the entire online payment process is conducted electronically and can be finalized in just a few seconds..

Due to its advantages, online payments have grown in popularity among consumers and sellers since the internet's inception. They enable customers to save a significant amount of time, which enables the procedure to be finished swiftly and effectively. Online payments enable consumers to conduct cashless purchases, eliminating the need for them to handle actual cash. By sending them a payment confirmation message, customers can purchase the products they want and pay for them with the highest level of security.

Online payment: what is it?

To put it simply, an online payment is an electronic monetary exchange that takes place over the internet.

When buying goods or services from suppliers, this online electronic payment is convenient.

Online payment apps facilitate online transactions between buyers and sellers. The transaction consists of the buyers purchasing goods and services and the sellers delivering those items or services. When transferring a buyer's money and a seller's goods, these simple online payment methods require a number of steps.

Types of Online Payment Methods:

The internet provides insights into the most effective online payment applications. Various online payment options have gained significant popularity, offering numerous advantages to users. Utilizing reliable platforms for online transactions is considered the safest and most efficient method for both buyers and sellers. Below are some of the prevalent types of online payments:

Credit Cards

Credit cards represent one of the primary sources of online payment methods. Using a credit card helps mitigate the risk of losses due to fraud. There are several types of credit cards available, including MasterCard, Visa, Discover, and American Express, all of which are widely used in India. Among these, MasterCard and Visa enjoy global acceptance, and each card type offers distinct benefits. Users can enjoy a range of advantages, such as travel insurance, rental car insurance, and purchase protection.

Debit Cards

Banks provide debit cards to their account holders as a component of their online payment services. These cards enable users to make purchases over the internet, with the corresponding amounts being automatically withdrawn from the cardholders' bank accounts. Much like credit card payment systems, debit card transactions are among the most favored online payment methods. The leading brands include Visa, RuPay, and MasterCard, with Visa cards being the most widely accepted by merchants globally for online and digital transactions. Debit cards offer a convenient solution for individuals looking to conduct online payments.

T Third-Party Payment Services

The most common method for online payments is through third-party transfers. This process involves issuing and depositing a payment into the account of an intermediary who facilitates the transaction. It is essential for users to understand how to execute payments online using this method.

Electronic Cheques

This digital payment method eliminates the necessity for users to write physical cheques, allowing sellers to deposit funds directly into their bank accounts. Compared to traditional paper cheques, electronic cheques offer enhanced security features, including verification, digital signatures, public key cryptography, and encryption.

Bank Transfers

Bank transfers operate similarly to debit card transactions. This method involves transferring funds from one bank account to another without the need for a physical debit card. Bank transfers are generally faster and more secure than other payment methods, such as cash withdrawals or direct payments from a bank account.Threats towards cyber security in online payments:

1) Malware

In the context of mobile payment security, malware poses a threat to smartphones, tablets, and similar devices by attempting to access sensitive information, including credit card details and account passwords. This malicious software can be disseminated through various means, such as harmful links sent via text messages, email attachments, or even through applications that are downloaded. Consequently, it is crucial for businesses to implement secure protocols when handling app downloads or opening links.

1) Phishing

The FBI reported that internet crime resulted in losses exceeding $4.2 billion in 2020, with phishing scams being the most prevalent issue faced by both individuals and businesses. Phishing represents one of the most widespread types of cyber-attacks and poses significant risks, especially regarding mobile payments. Typically, this scheme involves criminals sending fraudulent emails or text messages that mimic communications from legitimate entities, such as banks, online retailers, or payment processors. These deceptive messages often include links or attachments that lead the recipient to a harmful website, where they are prompted to input sensitive information, including credit card numbers or passwords.

2) Regarding online payments

Utilizing public Wi-Fi can present one of the gravest security threats for businesses. A recent survey indicated that 26% of respondents identified the use of public Wi-Fi as the primary vulnerability. Public Wi-Fi networks are generally open and lack security measures, allowing anyone to connect without needing to authenticate.

3) Identity Theft

Identity theft takes place when an individual acquires your personal information, including your name, address, social security number, bank account details, and other confidential data. With this information in hand, the identity thief can create new accounts under your name or unlawfully withdraw funds from your current accounts.

Objectives:

Integrity

- Establishing access control mechanisms through cryptographic methods
- Utilizing checksums or hashes
- Performing data backups and restorations
- Carrying out audits and evaluations

Availability

- Implementing redundancy and diversity strategies
- Utilizing load balancing and failover methods

- Executing patch management and configuration management processes
- Conducting testing and validation procedures
- Establishing service level agreements (SLAs)

Confidentiality

- Implementing encryption methods
- Utilizing authentication processes
- Applying authorization strategies
- Employing firewalls and network segmentation techniques
- Conducting risk assessments and classification procedures

Access Control

- Establishing identity management processes
- Utilizing password management tools
- Implementing multi-factor authentication techniques
- Employing role-based access control (RBAC) or attribute-based access control (ABAC) models
- Conducting access reviews and audits

Authentication

- Implementing biometric authentication methods
- Utilizing token-based techniques
- Applying knowledge-based methods
- Employing certificate-based techniques
- Conducting verification and validation procedures

Encryption

$ Implementing symmetric encryption techniques
Using asymmetric encryption techniques
Applying hybrid encryption techniques
g Employing key management processes
Conducting encryption testing and evaluation procedures

Compliance

$ Implementing governance frameworks
Using risk management processes
g Applying control frameworks
g Employing audit frameworks
Conducting compliance training

Incident Response

$ Implementing incident response plans
Using incident detection tools
Applying incident analysis techniques
$
g Employing incident containment strategies
2 Performing incident eradication actions
Conducting incident recovery steps

Security Architecture

$ Implementing security design principles
Using security development methodologies
g Applying security testing tools and techniques
g Employing security deployment practices
Performing security maintenance activities

Chapter: 02- LITERATURE REVIEW

Ana Rita D. Rodrigues, Fernando Teixeira, Fernando A. F. Ferreira, and Constantin Zopounidis (January 2022) highlight that the integration of new technologies into traditional banking transactions is currently experiencing significant demand from stakeholders. However, it is imperative that data security remains uncompromised, given the fundamental nature of the banking industry. The trust that customers place in their banking institutions is a vital element of the relationship between banks and their clients. A bank's reputation significantly influences its success, ability to attract new customers, and retention of existing clientele. These challenges complicate decision-making regarding the integration of cybersecurity, digital transformation, and artificial intelligence within the banking sector.

Leandre Gomes, Abhinav Deshmukh, and Nilesh Anute (2022) note that a growing number of individuals now favor E-banking, which has become an essential aspect of the financial ecosystem. While online banking offers numerous advantages to customers, they must remain vigilant to safeguard their accounts against hackers and cybercriminals, as online platforms are inherently susceptible to security threats. The internet security measures employed by most banking websites are often outdated compared to the rapidly evolving landscape of cyber threats. Consequently, this creates opportunities for hackers and other malicious entities to access sensitive financial information. Although various security precautions exist to prevent breaches, vulnerabilities within these systems persist.

R. P. Manjula and Dr. R. Shnumughan (2016) assert that the two primary principles governing real-time electronic surveillance in other criminal investigations are also applicable in this context. One of these principles involves the necessity of search warrants, which authorize law enforcement to enter locations believed to contain evidence of criminal activity. This includes the computer utilized in the commission of the crime, the software employed for unauthorized access, and other relevant evidence.

This study addresses the challenges and security issues related to digital banking. It explores various difficulties and security threats associated with online banking, including different fraud schemes, protective measures, and types of cyber-attacks that digital banks may encounter. The research focuses on the security and safety concerns surrounding internet banking.

We argue that addressing cybersecurity and e-commerce challenges through modern technology is a continuous struggle. To mitigate risks, it is essential to implement reliable technology, provide training for both customers and employees on technology usage, and establish comprehensive policies and regulations within organizations.□

Renata Marcinauskaite, Indre Pukanasyte, and Jolita Sukyte (2019) conducted a research study that explores various dimensions of unauthorized access to information systems (IS). This examination takes into account international treaties, European Union legislation, and relevant Lithuanian judicial precedents. The study delves into the elements constituting unauthorized access to an IS while addressing the challenges posed by terminology and technology. With the evolution of Lithuanian case law, there is an increased emphasis on the contentious breach of security protocols and its associated components.

Raheela Firdaus, Yang Xue, Li Gang, and Muhammad Sibt e Ali (2022) highlight the importance of this research for banks and their customers, particularly those who have been affected by cybercrimes. It is essential to reward honest employees and penalize dishonest behavior to deter individuals from exploiting such opportunities. Strict oversight is necessary, and all individuals must be held accountable for th eir roles. Skills should be utilized constructively, and ultimately, banks must effectively implement Artificial Intelligence to enhance transaction security.

The book by Dr. Erdal Ozkaya and Milad Aslaner (2019) begins with a comprehensive introduction to cyber-security, guiding readers through various critical services and technologies that are currently at risk of online attacks. As you progress through the chapters, you will encounter various flaws and vulnerabilities, including the human risk factor, providing insights from experts on the most recent threats.

Sarika R. Lohana (2020) discusses the vulnerabilities of cyberspace to a multitude of events, whether they are intentional or accidental, manmade or natural. Both nation-states and non-state actors can exploit the data shared in this environment for harmful purposes. Cyber-attacks pose risks to governments, corporations, and individuals alike. The only effective defense against such threats is to exercise caution with our data, preventing it from falling into the hands of fraudsters and scammers. This book addresses concerns related to cyber security and digital banking in a detailed and enlightening manner.

Shadi A. Alijawarneh (2016) notes that while technological advancements in the banking sector have greatly benefited both customers and banks, the rise of e-banking has also increased exposure to system threats and attacks, underscoring the necessity for robust security measures. This book is tailored for professionals, practitioners, advanced students, and technology developers who are keen on the latest developments in e-banking security. It introduces innovative strategies to protect these systems from potential threats and emphasizes both theoretical principles and practical case studies.

Kannan Balasubramanian, K. Mala, and M. Rajakan (2016) discuss the numerous positive changes in the electronic landscape that have emerged due to technological progress, especially in online commerce. Their work, "Cryptographic Solutions for Secure Online Banking and Commerce," addresses the challenges associated with securing online transactions and applications. This book serves as an essential resource for financial planners, scholars, researchers, advanced students, government officials, managers, and technology developers. It emphasizes research on various e-commerce protocols, including digital signatures, public key infrastructure, encryption algorithms, and digital certificates.

e The presence of numerous security issues represents a significant challenge associated with this form of banking. This research employs a theoretical analysis approach, utilizing secondary information sources, and has successfully formulated several hypotheses on the subject. These hypotheses are substantiated through statements and graphical representations from prior works by other authors in the field. The topic of this research is compelling and holds potential for further exploration in the future. Notably, a large segment of the population remains largely unaware of or indifferent to this issue.

Mrs. Kalpana Nayar and Priyanka Rathod (2021) define cyberspace as the digital domain of the Internet, governed by cyber laws that establish the framework for its regulation. Due to the quasi-universal jurisdiction of these laws, all internet users, referred to as netizens, are subject to them. Cybercrimes encompass activities such as hacking, phishing, and spamming, where computers are either the target or the means to perpetrate offenses, including child pornography and hate crimes. This phenomenon is often referred to as computer crime. Cybercriminals may exploit the internet to access corporate trade secrets, acquire personal data, or engage in malicious activities. This study specifically examines the cybersecurity challenges faced by Indian banks and assesses the general public's awareness of cybercrime.

Saqib Saeed, Salha A. Altamimi, Norah A. Alkayyal, Ebtisam Alshehri, and Dina A. Alabbad (2023) present a literature review that underscores the importance of comprehensively understanding cybersecurity risks during the implementation of digital transformation (DT). This understanding is crucial to prevent disruptions caused by malicious actions or unauthorized access by intruders aiming to manipulate, destroy, or exploit users. The article concludes by discussing potential future threats associated with DT adoption and offers recommendations for businesses to mitigate these risks through the establishment of robust cybersecurity measures, thereby preparing corporate organizations for the challenges ahead.

Tong Xin and Ban Xiaofang (2014) explore essential inquiries regarding the evaluation of security risks linked to online banking. Through this methodology, we develop the STRIDE threat model by analyzing significant business data pertinent to the online banking system, and we construct the threat tree through a systematic, layer-by-layer.

The dissection of security threats yields a comprehensive analysis of the risks associated with online banking platforms. This analysis is essential for recognizing the various threats confronting online banking and for evaluating the overall security of these systems.

According to research conducted by Victoria Wang, Harrison Nnaji, and Jeyong Jung (2020), the landscape of cybercrime in Nigeria has evolved from low-tech, cyber-enabled offenses to more advanced and sophisticated breaches. The three most prevalent types of breaches identified are hacking, infections from viruses, worms, or Trojans, and electronic spam. Banking personnel have received adequate management support and training regarding cybersecurity protocols.

In the study by Hemraj Saini, Yerra Shankar Rao, and T. C. Panda (2012), it is noted that online attacks can occur either inadvertently or with malicious intent. Cybercrimes are characterized as deliberate assaults that lead to significant societal disruptions, including economic instability, psychological issues, and threats to national security. To mitigate these crimes, a thorough analysis is necessary to comprehend their societal impacts. Consequently, this paper elucidates the nature of cybercrimes and their repercussions on society, while also offering insights into potential future trends in cybercrime.

Nir Kshetri (2019): Africa has emerged as one of the fastest-growing regions in terms of cybercrime activityHowever, considerable efforts have been made to strengthen cyber-security measures and address cyber threats across Africa. Many countries have implemented legislation aimed at combating these threats, and enforcement actions have been intensified. Furthermore, the private sector has taken initiatives to bolster cyber-security.

Dr. K. Sai Manoj (2020): "Banks are essential to the financial system and the economic development of a nation. The Indian banking sector is competing with global entities in the industry by focusing on customer service and improving efficiency through technological advancements. Financial institutions and online banking providers are acutely aware of the risks posed by cybercrime."

ac Various activities have led to the formulation of distinct legislations aimed at establishing a secure environment for banking and financial operations. Cyber-attacks pose a significant threat, potentially eroding customer trust in financial institutions. The challenge of cyber security is intricate and multifaceted, and its significance continues to escalate. This issue impacts not only banks but also governmental bodies. This research paper primarily examines the security dimensions of internet banking.

Recent studies indicate a dramatic increase in the number of IoT devices, with their usage becoming increasingly prevalent in daily life. Consequently, the imperative to secure these IoT devices is becoming ever more critical.

Johnny Rawass (2019) examined the methods employed by leaders of a small financial institution to safeguard their information systems against cyber threats, utilizing actor-network theory as the foundational framework for this research.

Jurjen Jansen and Eric Rutger Leukfeldt (June 2016) investigated the elements that may contribute to victimization in online banking fraud. This study applied the routine activity approach and protection motivation theory as its theoretical perspectives, drawing insights from 30 semi-structured interviews with individuals who experienced phishing and malware attacks.

Lenon Y.C. Chang and Nicholas Coppel (2020) argued that enhancing cyber-security awareness can bolster the resilience of productivity-boosting services, including mobile banking and e-payment systems, thereby fostering economic growth. They proposed a typology of cyber-security strategies that encompasses the roles of government, the private sector, and the international community.

M Ohamed Abomhara ; This growing prevalence has attracted attention, leading to a rise in threats and attacks targeting IoT devices and services. Although cyber-attacks are not a new phenomenon for IoT, their integration into our daily lives and societal structures necessitates a serious approach to cyber defense. Consequently, there is an urgent requirement to secure IoT, which underscores the importance of thoroughly understanding the threats and attacks that affect IoT infrastructure.

Munirul Ula, Zuraini BT Ismail, and Zailani Mohamed Sidek (2011) highlight that as contemporary banking becomes more dependent on the internet and computer technologies for its operations and market engagements, the incidence of threats and security breaches has significantly escalated in recent years. Both insider and outsider attacks have resulted in global businesses incurring losses amounting to trillions of dollars annually. Therefore, there is a pressing need for a robust framework to manage information security within the banking system.

2. Thanika Devi Juwaheer, Sharmila Pudaruth, and Priyasha Ramdin (2012) examine the factors that affect the adoption of internet banking services in Mauritius. Utilizing the technology acceptance model, the theory of reasoned action, the theory of planned behavior, and a comprehensive review of existing literature on the demographic characteristics of internet banking users, as well as the trust and security elements related to the adoption rates, this study integrates various established constructs into a single model. The constructs considered include perceived ease of use, perceived usefulness, subjective norms, awareness of internet banking services, and demographic factors such as age, income, gender, and education, all within a cohesive framework.

Chapter 03: RESEARCH METHODOLOGY

Research Objectives:

1. To evaluate the present condition of cyber-security within online banking and transactions, as well as to investigate the effects of cyber threats on these financial activities.
2. To analyze the effectiveness of existing security practices and measures, assessing their adequacy and efficiency in the context of online banking.
3. To identify optimal practices and strategies for improving cyber-security in online banking.
4. To explore the scope of the study focused on securing online payments and comprehending cyber threats while protecting financial transactions.

Cyber Threat Landscape Analysis:

1. Examine the current cyber threats aimed at online payment systems.
2. Identify new and evolving threats and trends in cybercrime associated with financial transactions.
3. Analyze various types of attacks, including phishing, malware, ransomware, and data breaches that target payment systems.

Payment System Architecture and Vulnerabilities:

1. Investigate the architecture of different online payment systems, such as credit card transactions, mobile payments, and cryptocurrency exchanges.
2. Identify vulnerabilities present in these systems, focusing on weaknesses in encryption protocols, authentication processes, and transaction handling.

Security Measures and Best Practices:

1. Review the security measures currently adopted by financial institutions, payment processors, and merchants to safeguard online transactions.

2. Assess the effectiveness of security protocols, including tokenization, multi-factor authentication, and end-to-end encryption.

Examine industry best practices for safeguarding online payments and reducing cyber threats.

Regulatory Compliance and Standards:
Evaluate the regulatory requirements and standards pertaining to online payment security.
Assess the challenges organizations encounter in meeting these compliance obligations.
Investigate the influence of regulatory agencies and industry associations in establishing standards for secure online transactions.

User Behavior and Awareness:
Analyze the influence of human factors on online payment security, focusing on user behavior and awareness.
Explore methods for educating consumers on safe online payment practices and increasing awareness of prevalent scams and fraud schemes.
Examine the effects of social engineering tactics on the security of online payments.

Technological Advancements and Future Directions:
1. Investigate new technologies and innovations in payment security, including blockchain, biometrics, and machine learning.
2. Evaluate the possible effects of technologies such as quantum computing on the security of online transactions.
3. Anticipate future developments in cyber threats and payment security, and suggest proactive strategies to mitigate them.

Case Studies and Incident Analysis:

1. Examine significant cyber incidents and data breaches related to online payment systems.
2. Explore the underlying causes of these incidents and the insights gained for enhancing payment security.
3. Review case studies showcasing effective security implementations and incident response tactics.

International Perspectives and Global Challenges:

- Consider the worldwide scope of online payment systems and the difficulties associated with cross-border transactions.
- Analyze the differences in payment security regulations and practices across various regions.
- Investigate international cooperative efforts aimed at addressing cyber threats within the financial industry.

Ethical and Legal Implications:

- Examine the ethical issues related to the collection and utilization of personal and financial information in online payment processes.
- Review the legal frameworks that regulate data protection, privacy, and cybersecurity concerning online financial transactions.
- Investigate the equilibrium between security protocols and the privacy rights of users.

Risk Management and Business Continuity:

- Explore risk management approaches for identifying, evaluating, and mitigating risks to online payment systems.
- Assess business continuity strategies and disaster recovery plans to maintain the robustness of payment infrastructure against cyber-attacks.
- Evaluate the financial and reputational consequences of security breaches for organizations and the wider economy.

The necessity of studying and comprehending cyber threats related to online payments and protecting financial transactions is paramount in today's digital landscape for several reasons:

- Increasing Cybercrime: As financial transactions become more digitized, cybercriminals are increasingly targeting online payment systems to acquire sensitive information, including credit card numbers, bank account details, and personal data.
- Financial Consequences: Cyber-attacks on online payment platforms can lead to substantial financial losses for both individuals and businesses, encompassing theft of funds and other related damages.

Fraudulent activities, the costs of rectifying compromised systems, and the associated risks are significant concerns. Trust and Confidence: The security of online payment systems is crucial for fostering trust and confidence among consumers. If users view these systems as unsafe, they may hesitate to utilize them, resulting in a decrease in online transactions and a negative impact on business revenue.

Legal and Regulatory Compliance: Companies that handle online payments must adhere to various legal and regulatory standards concerning data protection and cybersecurity. Non compliance with these regulations can lead to fines, legal action, and reputational harm.

New vulnerabilities and methods of attack are continually emerging, necessitating ongoing research and analysis to identify and mitigate potential risks to online payment systems.

Global Nature of E-commerce: Online payment systems function on a worldwide scale, making them appealing targets for cybercriminals aiming to exploit security weaknesses. Analyzing cyber threats in the realm of online payments enables businesses to recognize and address vulnerabilities across various regions and legal frameworks.

Emerging Payment Technologies: The advent of new payment technologies, including mobile wallets, cryptocurrencies, and biometric authentication, brings forth additional security challenges and potential vulnerabilities that require thorough examination and resolution.

Impact on Economic Stability: The security of online payment systems is vital for sustaining economic stability and preventing disruptions in financial markets. Cyber-attacks on payment infrastructures can have extensive repercussions, affecting businesses, consumers, and financial institutions alike.

Research Methodology

It encompasses a variety of techniques and procedures aimed at collecting and analyzing data to address research questions or evaluate hypotheses. The main objective of research methodology is to ensure that the research is executed in a manner that is valid, reliable, and generalizable. Validity pertains to the precision of the research outcomes, reliability relates to the consistency of the results, and generalizability indicates the extent to which the findings can be applied to other situations beyond the specific study.

Research Design:

This study employs primary research, utilizing questionnaires distributed to participants and relevant articles. The research design for this primary research study is outlined as follows:

- Research Questionnaire: Establishing the research questions that the study intends to address.
- Data Sources: The data sources consist of the responses provided by participants in the completed questionnaires.
- Data Collection: The systematic and thorough gathering and compilation of pertinent data from the identified sources.
- Data Analysis: The collected data will be analyzed using suitable qualitative analysis methods, such as content analysis, to uncover recurring themes and patterns.

Data collection procedure:

The procedure for gathering data entails a systematic method for acquiring information intended for research or analysis. It begins with the formulation of clear objectives and the identification of necessary data sources, which can include surveys, observations, interviews, or existing databases. To guarantee accuracy and relevance to the objectives, appropriate techniques are selected, and tailored instruments for data collection are developed.

Primary Data

Questionnaires serve as a tool for collecting primary data in research focused on cyber-security within online banking, targeting both users and institutions. These surveys yield initial information regarding user behaviors, perceptions of security, and issues related to transactions. They offer valuable insights into the complexities of cyber-security and highlight potential vulnerabilities by revealing experiences, opinions, and levels of trust in online platforms.

Secondary Data

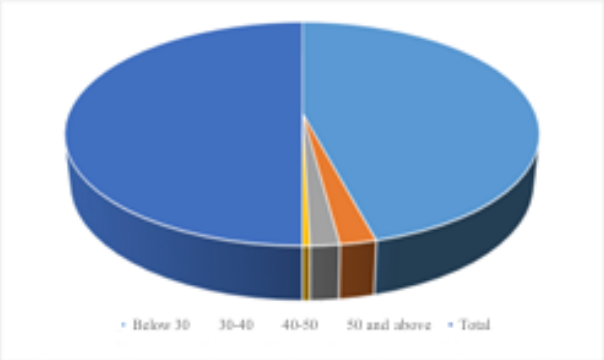
Research on cyber-security in online banking can greatly benefit from secondary data, which encompasses databases, research reports, case studies of cyber incidents, as well as books and academic journals. These resources aid in identifying vulnerabilities and understanding the broader landscape by supplying statistical information, prevalent threats, security measures, and insights into recent security breaches. They reveal patterns, statistical trends, and critical insights into the nature of cyber-security challenges. The combination of this data with primary sources enriches both the breadth and depth of the study.

Chapter 04: EMPIRICAL RESULTS AND INTERPRETATIONS

- Sampling Techniques:
  Selecting an appropriate sampling strategy is crucial when investigating cyber-security in online banking. Structured and random sampling methods ensure representation across various demographics and usage patterns. In contrast, convenience sampling, while quick, may introduce bias. Cluster sampling, on the other hand, effectively targets specific groups. These methodologies contribute to a deeper understanding of cyber-security challenges.

Frequency Table (age)

Particu ars	Frequency	percentage
ow I		
Bel 30	110	91.67
30-40	5	4.167
40-50	4	3.33
50 and above	1	0.83
Total	120	100

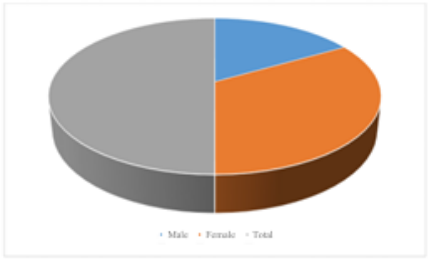


The provided data shows outlines the demographic distribution of sample population based on age. Majority of the respondents are of age below 30, constituting 91.67°/ of the sample,

The data presented illustrates the demographic distribution of the sample population according to age. A significant portion of the respondents, 91.67%, are under the age of 30. This is followed by individuals in the 30-40 age group, comprising 4.17%, those aged 40-50 at 3.33%, and finally, respondents aged 50 and above making up 0.83%.

Frequency Table (gender)

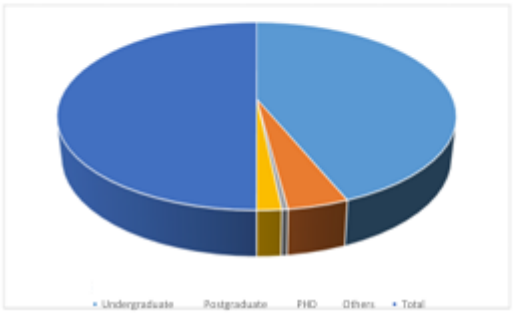
Particulars	Frequency	Percentage
Male	40	33.33
Female	80	66.67
Total	120	100



The data presented illustrates the demographic distribution of the sample population according to age. A significant portion of the respondents, 66.67%, are female, while males make up 33.33% of the sample.

Frequency Table (education level)

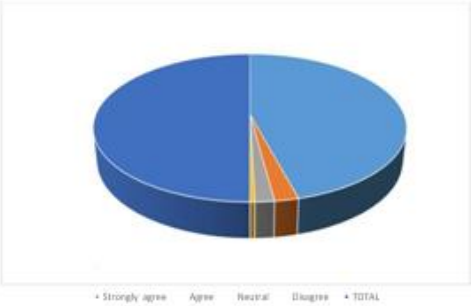
Particulars	Frequency	Percentage
Undergraduate	105	87.5 8.3
Postgraduate	10	0.83 3.33
PHD	1	100
Salaried person	4	
Total	120	



Data representation:

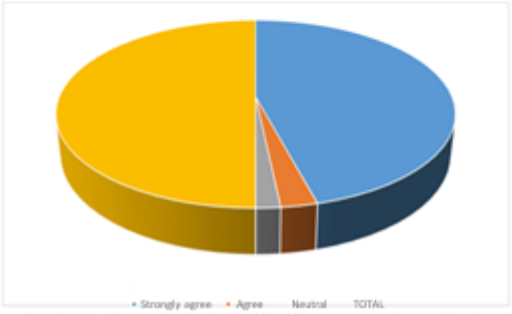
Respondents' opinions on using online banking services:

Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	110	91.67 4.167
2	Agree	5	3.33 0.83
3	Neutral	4	100
4	Disagree	1	
TOTAL		120	



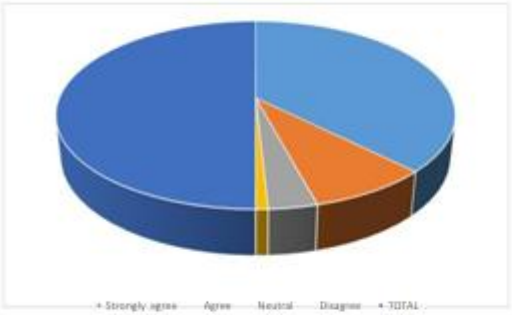
Respondents' opinions regarding potential cyber-security risks associated with internet banking are well-informed

Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	110	91.67
2	Agree	6	5
3	Neutral	4	3.33
TOTAL		120	100



Respondents' opinions on being careful while disclosing private banking information online.

Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	90	75
2	Agree	20	16.67
3	Neutral	8	6.67
4	Disagree	2	1.67
TOTAL		120	100

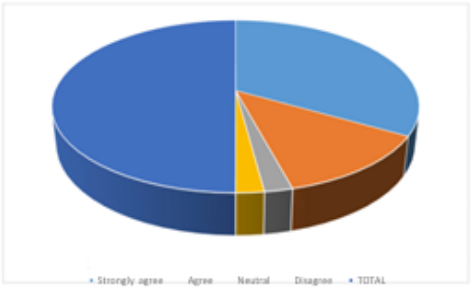


The provided data shows how respondents felt about the statement, "I am cautious about sharing personal banking information online." A substantial majority75°/ showed that they strongly agreed with the statement, which emphasises the need for extreme caution when disclosing personal banking information. Furthermore, 16.67°/ of respondents indicated agreement, indicating a strong general consensus regarding the significance of caution. Merely 1.67°/ disagreed with the statement, and only 6.67°/ of respondents were neutral. Remarkably, none of the respondents expressed strong disagreement.

These results highlight a general awareness and prudence among the respondents about sharing private banking information online, suggesting a generally responsible and watchful attitude towards protecting their financial information in the digital sphere.

The respondents' opinion of their awareness of the possible risks involved with utilising financial apps or services from third parties that connect to their online banking accounts.

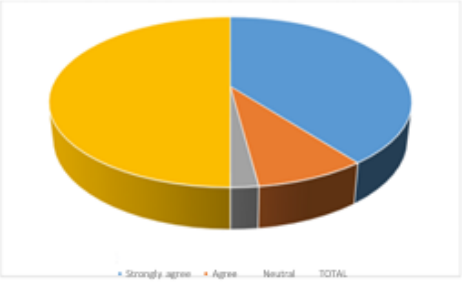
Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	80	66.67
2	Agree	30	25
3	Neutral	5	4.167
4	Disagree	5	4.167
TOTAL		120	100



The provided data shows the opinions of those surveyed regarding the claim that "I am aware of the potential risks associated with using third-party financial apps or services that link to your online banking account." Notably, 66.67% of respondents strongly agree with this statement, indicating that they are well aware of the possible risks involved in integrating their online banking accounts with third-party financial services. Furthermore, 25% indicate agreement, highlighting the broad agreement regarding the significance of comprehending these risks. 4.167% of respondents are neutral, and 4.167% disagree, and 0% strongly disagree. Overall, these results point to a general awareness among those surveyed of the possible dangers connected to third party financial apps or services that are connected to online banking.

Based on respondents' opinions, financial institutions ought to give customers ' privacy more weight than the gathering of data for security purposes.

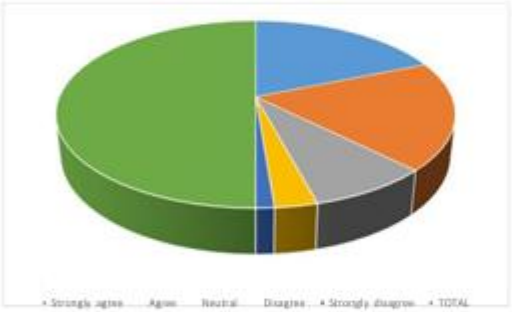
Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	95	79.167
2	Agree	20	16.67
3	Neutral	5	4.167
TOTAL		120	100



79.167% of respondents strongly agree with this viewpoint, indicating a strong belief in the importance of protecting customer privacy over gathering a lot of data for security reasons. Furthermore, 16.67% of respondents indicate agreement, demonstrating a strong consensus regarding the significance of prioritising customer privacy. The remaining 4.167% are neutral, suggesting that some respondents had no strong feelings about the issue. Remarkably, none of the respondents disagreed or strongly disagreed. Overall, these results point to a widely held belief in the importance of protecting personal data while putting security measures.

Respondents' opinions on using antivirus or extra security software in particular to protect online banking activity.

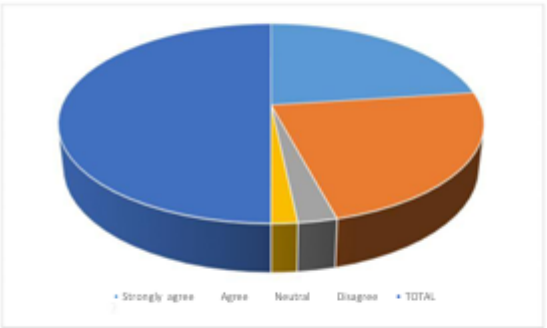
Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	45	37.5
2	Agree	45	37.5
3	Neutra l	20	16.67
4	Disagree	7	5.83
5	Strongly disagree	3	2.5
TOTAL		120	100



37.5% of respondents strongly agree and agree that using extra security measures to protect their online banking is a good idea. This suggests that a sizeable percentage of the respondents are actively working to improve security. Moreover, 16.67% are neutral, indicating a sizable portion that has neither a strong preference for nor against the use of additional security software. All told, 5.83% disagree with the statement, with and 2.5% strongly disagreeing. This suggests that there may be a minority of people who do not think highly enough of extra security measures designed especially for online banking. Overall, these results point to a varied but generally proactive attitude towards online banking security.

The opinions of respondents indicate that they think online banking platforms ought to offer their customers additional instructional materials regarding cyber- security.

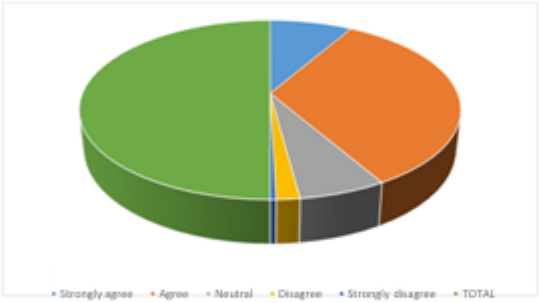
SI. No.	Responses	Frequency	Percentage
	trongly agree		
1	Sgree	55	45.83
2	Aeutra	55	45.83
3	Nisagree	6	5
4	D	4	3.33
TOTAL		120	100.00



A sizable fraction, 45.83% , strongly agree and agree with this statement, suggesting that there is a general consensus among those polled regarding the need for online banking platforms to step up their efforts to offer cyber-security education. Furthermore, 5% are neutral, indicating a tiny percentage that has no strong feelings about the issue. However, 4% disagree, highlighting a minority opinion that might not give priority to the requirement for more cyber-security education materials from online banking platforms. Interestingly, none of the respondents strongly disagree. Overall, these results point to a strong desire for better cyber-security education programmes, demonstrating a shared understanding of the value of providing users with the information they need to increase their awareness of online security.

According to respondents, banks disclose potential hazards and weaknesses in their online banking systems in a sufficiently open manner.

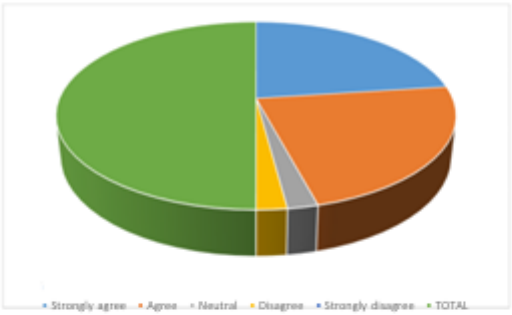
Sl.no.	Responses	Frequency	Percentage
1	Strongly agree	20	16.67
2	Agree	80	66.67
3	Neutral	15	12.5
4	Disagree	4	3.33
5	Strongly disagree	1	0.83
TOTAL		120	100



A significant proportion 16.67% express strong agreement, of which 66.67% agree. This suggests that banks are transparent in disclosing potential risks and vulnerabilities in their online banking systems. Moreover, 12.5%Zoare neutral, indicating a sizable portion of the population that has no strong feelings about banks' transparency in this area. With 3.33%Zo disagreeing and 0.83%Zostrongly disagreeing with the statement. This suggests a minority opinion according to which banks do not disclose enough information about the dangers and weaknesses in their online banking systems.

Based on respondents, utilizing two-factor authentication for online banking is worthwhile since it adds an extra degree of security.

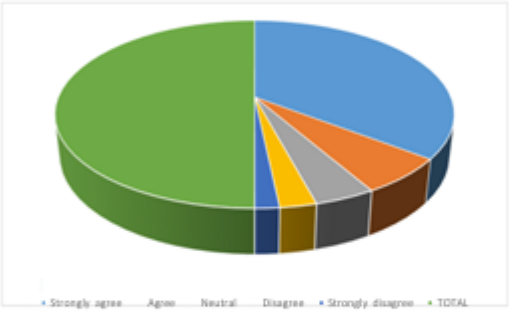
Sl.no	Responses	Frequency	Percentage
1	Strongly agree	55	45.83
2	Agree	55	45.83
3	Neutral	5	4.167
4	Disagree	5	4.167
5	Strongly disagree	0	0
TOTAL		120	100



A sizable majority of 45.83%Zorespondents strongly agree as well as agree with the statement, demonstrating the general consensus regarding the usefulness and effectiveness of two-factor authentication in boosting the security of online banking transactions. Furthermore, 4.167%Zoof respondents are neutral, indicating that there is a minority that has no strong opinions on the subject and 4.167%Zodisagree. Overall, these results show that there is broad agreement among those surveyed about the value and efficiency of adding two-factor authentication to online banking as an extra security measure.

Respondents' opinion regarding likelihood of implementing new security measures offered by banks to improve security of online banking.

Sl. No.	Responses	Frequency	Percentage
1	Strongly agree	85	70.83
2	Agree	15	12.5
3	Neutral	10	8.33
4	Disagree	6	5
5	Strongly disagree	4	3.33
TOTAL		120	100



This statement was endorsed by 70.83% of participants strongly agree, 12.5% agree. This suggests that the surveyed individuals are very willing to accept and adopt new security measures that banks have put in place to improve the security of online banking. Furthermore, 8.33% are neutral, indicating a smaller percentage with no strong preference in either direction. In contrast, 5% disagree with the statement and 3.33% strongly disagreeing. This suggests a minority viewpoint that might be less likely to quickly accept newly implemented security measures by financial institutions. Overall, the data shows that the surveyed group was generally open to accepting new security initiatives that banks were introducing to increase the security of online banking transactions.

Findings

- The study on cyber security issues affecting online banking and transactions, which utilized a questionnaire distributed to respondents, yielded several key findings. Below is a visual summary of these findings:

- Significant participation in online banking: A large majority of respondents strongly affirm their engagement in online banking activities, indicating a broad acceptance of these services.
- Gender equality in online banking usage: Although the majority of respondents are female, there is no notable difference in their level of agreement regarding online banking security compared to their male counterparts. This implies that both genders share similar concerns and awareness of cyber-security threats in online banking.
- Recognition of cyber-security threats: A considerable number of respondents express strong agreement about their awareness of potential cyber-security risks linked to online banking, indicating a generally knowledgeable user demographic.
- Concerns about privacy: Respondents exhibit significant apprehension regarding the sharing of personal banking information online, with many strongly agreeing that they exercise caution in this area.
- Awareness of risks from third-party applications: The majority of respondents acknowledge the potential dangers associated with using third-party financial applications or services linked to their online banking accounts, reflecting a prudent attitude towards such integrations.
- Emphasis on customer privacy: Respondents strongly believe that financial institutions should prioritize customer privacy over extensive data collection for security purposes, highlighting a preference for safeguarding personal information.
- Endorsement of security enhancements: There is a general consensus among respondents in favor of implementing additional security measures, such as antivirus software and two-factor authentication, to bolster online banking security.
- Demand for education and transparency: Respondents express a strong desire for online banking platforms to provide additional educational resources and transparency regarding security practices.

1. Acceptance of new security initiatives: most respondents are open to accepting new security measures introduced by banks to improve online banking security, suggesting a willingness to adapt to evolving security protocols.
2. Desired for enhanced cyber-security education: there is a strong desire among respondents for online banking platforms to offer additional instructional materials regarding cyber-security. This indicates a strong recognition of the importance of user education in mitigating cyber-security risks and suggests an opportunity for financial institutions to enhance their educational resources and initiatives in this area.

Chapter 05: Conclusion and Recommendations

The reliability and security of online banking and transactions face ongoing challenges due to cyber-security threats. A variety of risks exist, ranging from sophisticated phishing schemes to insidious malware and data breaches. Phishing attacks deceive individuals into revealing personal information through fraudulent emails or websites. Malware, including ransomware, can infect devices, leading to financial theft or the hijacking of computers. Data breaches compromise the confidentiality of personal information, increasing the risk of fraud and identity theft. These threats not only result in significant financial losses for individuals and businesses but also undermine the trust that is fundamental to online banking systems.

Public collaboration is crucial in the fight against these security threats. It is imperative for users, regulatory bodies, cyber-security experts, and financial institutions to unite. Key components of this collaboration include sharing threat intelligence, implementing regulatory frameworks, and fostering innovation. Stringent regulations ensure compliance with security standards, thereby strengthening the online transaction landscape. Continuous innovation in security technologies and processes is vital to keep pace with the evolving tactics employed by cybercriminals. By working together, we can establish a resilient environment that deters cyber-attacks and enhances trust in online banking services. Ultimately, a comprehensive strategy is essential for mitigating cyber-security threats in online banking and transactions. This strategy must encompass a solid technological foundation, user education, and collaboration among stakeholders. In an increasingly interconnected and vulnerable world, the integrity, confidentiality, and reliability of digital financial transactions can only be safeguarded through a coordinated effort.

Recommendations:
Ongoing education and awareness: Establish and execute extensive educational initiatives aimed at informing online banking users about cyber-security threats and effective practices. These initiatives may encompass informational materials, webinars, workshops, and interactive tools designed to assist customers in recognizing and addressing potential risks. Transparency and communication: Financial institutions must emphasize the importance of transparency and maintain open lines of communication with customers concerning the security protocols in place.

- place and any potential risks associated with online banking. This can include regular update on security protocols, data breaches and proactive measures taken to safeguard customer information. Privacy protection: strengthen privacy policies
- and practices to prioritize the protection of customer data. This can involve implementation of data encryption methods, ensuring secure storage and transmission of sensitive information, and adhering to strict privacy regulations and standards. Customised security options: offer customers a range of security
- options and features tailored to their preferences and needs. This might include multi-factor authentication methods, biometric authentication, real-time transactions monitoring, and personalised security alerts to help customers proactively manage their online banking security.

References

Borgave, S. (2022). An Examination of Cyber Security Challenges in Online Banking and Transactions. Neuro Quantology, 20(18), 405.

Kali, M. A., & Akter, N. (2023). Protecting Financial Data in the Digital Age: Case Studies on Cyber Security for Accounting Information Safeguarding. American Journal of Trade and Policy, 10(1), 15-26.

Ghelani, D. (2022). Cyber Security: Threats, Implications, and Future Outlooks: A Comprehensive Review. Authorea Preprints.

Vishnupriya, N., & Bhujanga, D. An Investigation into Cyber Security Challenges Impacting Online Banking and Transactions.

Rawass, J. (2019). Strategies for Cyber Security to Safeguard Information Systems in Small Financial Institutions (Doctoral dissertation, Walden University).

Chen, Y. (2018). Assessing Security Risk Tolerance in Mobile Payments: A Trade-Off Framework. Old Dominion University.

Josyula, H. P., Reddi, L. T., Parate, S., & Rajagopal, A. (2024). A Review of Security and Privacy Issues in Programmable Payments. International Journal of Intelligent Systems and Applications in Engineering, 12(9s), 256-263.

- Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Albanna, A. (2023). Online Banking User Authentication Methods: A Systematic Literature Review. IEEE Access.
- Alodhiani, A. A. B. (2023). Financial Technology (Fintech) and Cyber-security: A Systematic Literature Review.
- Badotra, S., & Sundas, A. (2021). A systematic review on security of E-commerce systems.
- Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis. ILEE Access.
- Manoj, K. S. (2021). International Journal o1 Management (IJM), 12(1), 1332-1339.
- Dursunzade, O. (2021). Assessment of Security Threats on IOT Based Applications: Cyber Security Case Study in Cloud-Based IOT Environment Using the Example of Developing Cloud Information Security Technology in Banking (Doctoral dissertation).
- Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security, 97, 101959.
- Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Security. Mobil. 4(1), 65-88.