CYBERSECURITY IN BANKING: INTEGRATING BIOMETRICS AND THREAT CLASSIFICATION

TECHNICAL SEMINAR REPORT

By

G MADHUMATHI

(Register No: 9517202352025)

of

MEPCO SCHLENK ENGINEERING COLLEGE, SIVAKASI

Submitted to the

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment of the award of degree of

MASTER OF COMPUTER APPLICATIONS

ANNA UNIVERSITY, CHENNAI

JUNE 2025

CERTIFICATE

This is to certify that the Technical Seminar report titled **"Cyber security in Banking: Integrating Biometrics and Threat Classification"** is a bonafide record of the seminar work submitted by **Ms. MADHUMATHI G** (Register Number: **9517202352025)** of MCA, submitted in partial fulfillment of the requirements of the course 23CA451 – TECHNICAL SEMINAR during the academic year 2024–2025.

Supervisor
Dr. A.D.C.Navin Dhinnesh
Associate Professor
Department of Computer Applications
Mepco Schlenk Engineering College
Sivakasi.

Director
Dr. P. RADHA
Professor & Director
Department of Computer Applications
Mepco Schlenk Engineering College
Sivakasi.

Research Paper I

Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis

ABSTRACT

In the digital era, cyber security threats have become increasingly sophisticated, posing significant challenges to personal privacy, financial security, and institutional integrity. The banking sector, in particular, has witnessed a surge in cyber threats due to the growing reliance on online financial transactions. This paper examines the integration of biometric authentication systems as a critical countermeasure to these emerging cyber security risks. The study highlights the increasing interest in biometric systems across various sectors, including private, public, and corporate domains, with a particular focus on their application in both conventional and Islamic banking systems. Through a systematic literature review of 101 peer-reviewed articles published between 2009 and 2023, the research identifies trends, challenges, and advancements in the use of biometric technologies to mitigate cyber threats. Key biometric modalities such as fingerprint scanning, facial recognition, iris detection, and voice analysis are evaluated for their effectiveness in protecting online banking platforms from fraud and unauthorized intrusions. The paper also addresses the broader implications of cybercrime, including its impact on data privacy, financial loss, and national security. It emphasizes the vulnerabilities of Internet of Things (IoT)-based banking systems and the growing role of Artificial Intelligence (AI) in both cyber security defence and potential threat scenarios. The integration of biometric systems with AI-powered analytics is explored as a promising solution to enhance real-time threat detection and adaptive security measures. Overall, the paper underscores the importance of biometric authentication as a strategic component in strengthening cyber security frameworks within the banking sector. By combining advanced biometric verification with robust cyber security protocols, financial institutions can significantly reduce the risk of cyber-attacks, ensure secure banking experiences, and maintain customer trust in an increasingly digitized financial ecosystem.

Research Paper II

Cyber Threats Classifications and Countermeasures in Banking and Financial Sector

ABSTRACT

The banking and financial sectors are prime targets for cyber threats due to the critical and sensitive nature of the information they manage. With increasing reliance on digital technology and transformation, these sectors face increasingly complex and sophisticated cyber-attacks. As the backbone of the economy, any disruption in banking can significantly impact other industries and the overall economic stability. This paper provides a comprehensive analysis of cyber threats in banking and finance, focusing on identifying common threats, their characteristics, and classifying them based on severity and technical complexity. This classification aids in determining effective countermeasures to mitigate risks. The research also explores technical, organizational, legal, and regulatory measures designed to protect financial transactions from cyber threats. Additionally, it discusses the challenges posed by the rapidly evolving cyber threat landscape and highlights recent trends in cyber security for the banking sector.

ACKNOWLEDGEMENT

I am in great pleasure to acknowledge all those who generously helped me in completing the technical seminar. First I thank almighty God for his sustained blessings at all stages of my technical seminar.

I can hardly find words to express my gratitude to the care and encouragement that received from my beloved **Parents**.

I express my sincere gratitude to **Dr. S. Arivazhagan, M.E., Ph.D., Principal,** Mepco Schlenk Engineering College, for giving me this opportunity to carry out this technical seminar.

My sincere and special thanks to **Dr. P. Radha, M.Sc.,M.Phil.,Ph.D., Director**, Department of Computer Applications for her charming interest and guidance in the technical seminar and a special thanks to all staff members of our department.

I have great pleasure in conveying my heartfelt thanks to my internal guide **Dr. A.D.C. Navin Dhinnesh, Associate Professor,** Department of Computer Applications for his guidance in finishing the technical seminar.

Finally, I would like to thank all those who directly and indirectly helped me in the successful completion of the technical seminar.

TABLE OF CONTENT

LIST OF FIGURES

Research Paper I: Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis

CHAPTER - 1
INTRODUCTION

Cybercrime has become one of the most pressing challenges in today's digital age, especially for sectors that deal with sensitive data like banking. Unlike traditional crimes, cybercrimes are carried out through the internet and information technologies, making them harder to track and more damaging. In many developing countries, the rising number of cyber-attacks has made it increasingly difficult for banks and financial institutions to maintain trust and security.

Over the past few years, the global banking sector has faced serious disruptions - not just from economic crises, but also from sophisticated cyber threats. These incidents have led to a noticeable loss of customer confidence, pushing banks to rethink how they protect customer data and maintain operational stability. Amid this evolving threat landscape, biometric technology has emerged as a powerful tool to enhance cyber security. By using physical traits like fingerprints, facial features, and iris patterns, biometrics provides a more reliable way to verify identity and prevent unauthorized access.

The paper chosen for this seminar explores how biometric systems can strengthen cyber security in the banking industry. It argues that with most banking services now hosted on the cloud, protecting data is no longer just about strong infrastructure, but about having smarter access control systems—ones that include artificial intelligence, two-factor authentication, encryption, and authorization.

The study also points out that as banks try to grow and adapt in a highly competitive and globalized environment, cyber security needs to be a top priority. Recent technological advancements like AI, Big Data, IoT, block chain, and machine learning are transforming the financial sector. While these tools bring efficiency and innovation, they also open new doors for cybercriminals.

Modern banking systems are constantly under threat from cybercrimes like phishing, ATM frauds, identity theft, and denial-of-service attacks. Some financial

institutions have started using a combination of biometrics and multi-factor authentication to create stronger, more secure systems. Others are leveraging data mining and analytics to detect fraud, understand customer behavior, and make smarter financial decisions.

This paper aims to:

- Identify major cyber security challenges faced by the banking and finance industry;
- Explore practical solutions and suggest future directions for research;
- Improve current security systems by integrating advanced biometric approaches;
- Explain the key benefits of using biometric systems to reduce cybercrime in banking.

By looking closely at these aspects, the paper offers valuable insights into how biometric technology can play a central role in protecting both financial institutions and their customers in a fast-changing digital world.

CHAPTER - 2
LITERATURE REVIEW

Islamic finance and capital markets represent one of the fastest-growing segments of the global financial industry. Driven by innovations in financial instruments and evolving regulatory frameworks, the landscape of Islamic banking has undergone significant transformation. Over the past two decades, it has witnessed unprecedented growth, emerging as a viable alternative for both investors and depositors worldwide. Despite its expansion, Islamic banking faces critical challenges—most notably, ensuring Shariah compliance in interest-dominated financial environments, particularly within Muslim-majority countries.

A second major concern lies in how professionals within the financial sector perceive the operational performance of Islamic banking and whether it effectively meets modern industrial and commercial demands. Additionally, there is an ongoing debate among Muslim consumers regarding the authenticity of Islamic financial practices—questioning whether these services genuinely align with Shariah principles or merely replicate conventional Western banking models under a religious label.

The rapid development of FinTech—a blend of finance and technology—has also had a substantial impact on Islamic finance. Like Islamic banking, FinTech has grown rapidly over the last decade, offering innovative solutions while adhering to Shariah guidelines. The core mission of Islamic FinTech is to drive inclusive social and economic development through Shariah-compliant tools. The Financial Stability Board defines FinTech as “technologically enabled financial innovation that could result in new business models, applications, processes, or products with a material effect on financial markets and institutions.”

Alongside these developments, cybersecurity has emerged as a central concern. With the increasing adoption of online services—commonly referred to as "cyber banking"—cyber threats have become more sophisticated and widespread. These threats are often described as a form of financial terrorism, targeting user data and disrupting banking operations globally. Despite the enhanced convenience offered by digital banking platforms, maintaining user privacy remains a formidable

challenge. As new technologies arise, so do vulnerabilities, highlighting the urgent need for robust cyber security strategies.

Biometric authentication has gained traction as a promising solution in cyber security. Facial recognition systems, for instance, identify individuals based on their unique facial features and are now used in contexts ranging from law enforcement to mobile banking. Although various security protocols are currently in place, vulnerabilities persist across digital infrastructures. Financial institutions must develop predictive models and implement continuous, intelligent monitoring systems to detect and prevent cyber threats effectively. Such resilience can only be achieved through the integration of advanced, cyber-resilient technologies.

While biometric security systems greatly reduce the likelihood of breaches compared to traditional password-based systems, they are not entirely foolproof. Attackers can still exploit hardware vulnerabilities, even in high-quality biometric devices. Therefore, cyber security measures must evolve continuously to defend against increasingly complex threats. Protecting against cyber-attacks is not only a matter of financial security but also of maintaining public trust.

In recent years, technologies such as Artificial Intelligence (AI), Big Data, 5G, and IoT have significantly reshaped the financial landscape. Major financial institutions are increasingly integrating these technologies to enhance service delivery and strengthen digital defenses. AI, in particular, is being used across various sectors—including finance, manufacturing, education, and government—to improve decision-making and service efficiency. Its application in public safety, such as in criminal identification and fraud detection through biometrics, highlights its potential to drive transformative change.

CHAPTER - 3
SYSTEM METHODOLOGY

The research employed a Systematic Literature Review (SLR) methodology to thoroughly analyze various cyber-attacks targeting the banking sector. The SLR method is defined as a rigorous approach to identifying, interpreting, and evaluating all existing research related to a specific topic or research questions (RQs). Unlike ad hoc literature reviews, SLR ensures a comprehensive and unbiased coverage of relevant high-quality papers, minimizing selective reporting or partial evaluation of findings.

The SLR process in this study involved three primary phases: planning, conducting, and reviewing. A review paradigm was developed during the planning phase to guide the subsequent steps and mitigate researcher bias. This paradigm outlined the research questions, topic selection criteria, search strategies, article evaluation standards, and data synthesis procedures.

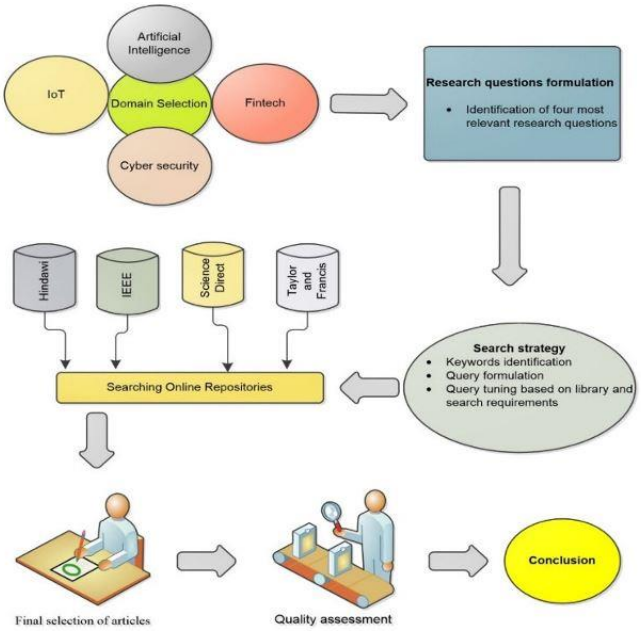

Figure 3.1 Process adopted for SLR

A. Research Domain Selection

To gain a comprehensive understanding of cyber security challenges in the banking industry, relevant literature was surveyed extensively. This involved

analyzing scholarly works from multiple digital information sources to identify existing problems and solutions related to biometric systems and cybercrime prevention in financial organizations.

B. Formulation of Research Questions

Figure 3.2 represents the formulation of research questions. Four primary research objectives guided this study: (1) to identify key biometric technologies affecting banking cyber security; (2) to examine the influence of biometric systems and FinTech on the financial sector; (3) to highlight benefits experienced by the banking industry through biometric adoption; and (4) to explore enhancements for current systems to improve protection against cyber-attacks.

S.No	RQs	Explanation
Q1.	What are the key features of biometrics system that affect banking and prevent cyberattacks?	The purpose of this question is to describe the various features that can affect banking to prevent cybersecurity by utilising the biometrics system.
Q2.	How does cybercrime influence FinTech in the banking sector?	FinTech is an emerging technology that can influence the banking sector. The aim of the research question is to secure the transaction between the parties by using financial technology and its features.
Q3.	What are the key benefits gained by the banking sector using biometric systems after overcoming cyberattacks?	As the banking sector shifts its business from a traditional to a modern global environment, the risk of cyberattacks and cybercrime is increasing day by day. The aim of this RQ is to provide smooth and secure operations by using biometrics technology to overcome the risk of cyberattack.
Q4.	Using the literature as evidence, how can we enhance the competence of the existing system to secure the banking sector?	By overcoming cyberattacks, what are the major benefits brought to financial organisations? This RQ aims to enhance the competencies of existing available systems to secure the banking sector, enhance customer satisfaction and trustworthiness levels, and build a bridge between banks and clients.

Figure 3.2 Formulations of Research Questions

C. Search Strategy

A string-based keyword search was formulated using Boolean operators to cover the relevant terminology. The constructed query included terms such as “biometrics,” “fingerprint,” “face recognition,” “cybercrime,” “fraud,” “cyber security,” and “banking sector,” combined logically to capture a wide range of relevant studies.

D. Searching Process

The literature search was conducted across four leading digital libraries: IEEE Xplore, Science Direct, Hindawi, and Taylor & Francis. The process consisted of three phases: initially scanning for publications relevant to the topic; mining articles based on the keyword string; and extracting pertinent studies from the digital repositories. To avoid duplication, metadata was cross-checked and articles were carefully filtered. Figure 3.3 illustrates the details of selected paper:

	IEEE Xplore	Science Direct	Hindawi	Taylor & Francis
Conferences	334	44	8	-
Journals	19	333	316	286
Books	21	11	-	15
Magazines	8	-	-	-
Books Chapters	-	97	-	-
Case report	-	-	93	-
case series	-	-	13	-
Editorial	-	-	71	4
Others	-	-	44	19

Figure 3.3 Details of selected paper

E. Scrutinization and Retrieval

The initial search yielded 1,283 articles. Titles, abstracts, and keywords were reviewed manually to exclude irrelevant or duplicate studies. This screening narrowed the set to 101 relevant publications for further evaluation.

Online databases	Filter by keywords based	Filtered by title	Filter by abstract	Filter by contents
Hindawi	7659	279	98	23
IEEE Xplore	11715	301	114	32
Science Direct	13472	332	125	25
Taylor	9761	371	132	21
Total	42607	1283	469	101

Figure 3.4 Selection of Primary Research

F. Quality Assessment and Data Synthesis

Each of the 101 selected articles was assessed based on its ability to address at least two of the formulated research questions. A binary scoring system was used, where “yes” equaled 1 and “no” equaled 0 for each question. Studies scoring below the threshold were excluded, resulting in 61 papers being discarded. The final selection comprised studies that sufficiently answered the research questions, ensuring a high-quality dataset for synthesis.

The data extracted from these studies enabled detailed insights into biometric characteristics influencing banking security, FinTech’s impact on financial services, benefits gained through biometric system integration, and proposed enhancements to existing cybersecurity frameworks.

CHAPTER - 4
RESULTS AND INFERENCES

The following section addresses the key research questions by summarizing relevant findings from the literature.

RQ1: Key features of biometric systems in Banking

Cybercrime remains a growing concern globally, particularly in developing countries, where rapid digital adoption often outpaces security measures. Biometric authentication methods—such as fingerprint scanning, facial recognition, and iris scanning—offer enhanced security by relying on unique physiological traits that are difficult to replicate or steal. When combined with artificial intelligence, biometric systems can detect anomalies and prevent unauthorized access more effectively. Key features that impact banking security include multi-factor authentication capabilities, real-time threat detection, and user-friendly interfaces that promote adoption without compromising security. These features collectively help banks reduce fraudulent activities and increase customer trust.

RQ2: Cybercrime's impact on FinTech in Banking

FinTech has transformed the financial services landscape by introducing innovative solutions that increase transaction speed, reduce costs, and improve accessibility. However, the rapid expansion of FinTech also introduces new cyber security challenges. Cybercriminals exploit regulatory gaps, especially where FinTech companies operate with less oversight than traditional banks. Activities such as money laundering, identity theft and financial fraud are significant threats that accompany the growth of FinTech. Despite these risks, FinTech continues to grow, driven by advances in technology like block chain, AI, and big data analytics, which offer promising tools for improving security. Additionally, the widespread adoption of smartphones and affordable internet connectivity, particularly in countries like India, has accelerated FinTech penetration and highlighted the importance of robust cyber security frameworks.

RQ3: Benefits of Biometrics for banks

The adoption of biometric systems in banking has led to several key benefits. Firstly, these systems significantly reduce the incidence of fraud by providing a reliable way to verify user identities. Secondly, they enhance the overall customer experience by simplifying login and transaction authentication processes. Thirdly, biometric authentication lowers operational costs related to password management and fraud investigation. Lastly, by increasing security and reducing breaches, banks can improve customer confidence in digital platforms, leading to greater adoption of online and mobile banking services.

RQ4: Enhancing existing security systems

While laws like electronic signature regulations help improve security for online banking, they aren't enough on their own to stop cyber-attacks. To really protect banking systems, we need a layered approach that combines strong laws, new technology, and educating users. This means using advanced biometric tools (like fingerprint or face recognition), constantly monitoring activities with smart AI systems, encrypting data, and making sure transactions are secure. Regulators also need to keep updating rules to keep up with new threats and make sure FinTech companies follow them. On top of that, teaching customers how to stay safe online is important to reduce risks. By working on all these fronts together, banks can better defend against cybercrime and provide safer, more reliable services.

CHAPTER - 5
CONCLUSION

This study highlights the critical role of biometric systems in strengthening cyber security within the banking sector. Despite some customer inconvenience due to repeated identity verification, biometric authentication is essential to combat increasing identity theft and cyber fraud. Banks are adopting biometric technologies such as fingerprint, facial, and voice recognition to secure mobile apps and online transactions. The combination of AI and biometrics enhances fraud detection capabilities and helps prevent cyber-attacks more effectively.

Moreover, the continuous digital transformation in banking requires evolving security solutions to address emerging threats, including AI-powered deepfakes. Maintaining high data security is vital for preserving customer trust, protecting bank reputations, and ensuring regulatory compliance. As cyber threats grow more sophisticated, a proactive and multi-layered defence approach that combines legal frameworks, technological innovation, and customer education becomes indispensable.

Future efforts should focus on improving biometric accuracy and user experience to minimize inconvenience while maximizing security. Additionally, collaboration between financial institutions, technology providers, and regulatory bodies will be key to establishing robust standards and timely responses to new cyber risks. By integrating advanced biometric and AI-driven systems with comprehensive policies and awareness programs, banks can build resilient ecosystems that deliver secure, reliable, and user-friendly financial services, fostering long-term trust and stability in the digital economy.

Research Paper II: Cyber Threats Classifications and Countermeasures in Banking and Financial Sector

CHAPTER - 1
INTRODUCTION

The banking and financial sector is at the heart of the economy, and over the past decade, it has transformed dramatically thanks to digital technology. While this shift to online and mobile banking has made services more accessible and convenient, it has also opened the door to new and increasingly complex cyber threats. Cybercriminals are constantly coming up with smarter ways to attack banks, which can lead to huge financial losses, damage to reputation, and even legal troubles for these institutions. Because banks are connected to many other industries, a major cyber-attack on them could ripple through the entire economy.

There have been several high-profile attacks in recent years—from ransom ware hitting banks to data breaches exposing millions of customers' personal information. The costs of these attacks are staggering, with millions of dollars lost per incident and a sharp increase in phishing and ransom ware attacks. Because banks face such high risks, it's vital they put strong cyber security measures in place. This means not only using technical tools like firewalls and intrusion detection systems but also adopting organizational policies and legal protections.

This research aims to better understand the common cyber threats facing banks, how to classify them by their risk level and complexity, and what steps can be taken to protect against them. The two main questions it focuses on are:

- What types of cyber threats do banks and financial institutions face, and how can these threats be categorized?
- What technical and organizational measures can help reduce the risks from these threats?

CHAPTER - 2
LITERATURE REVIEW

Numerous studies have examined cyber threats targeting the banking and financial sectors. Shkodinsky provided a critical overview of both domestic and international research, offering practical recommendations to protect banking institutions in the digital economy. Building on this, Yevseiev and colleagues proposed an advanced classification system for threats to banking information resources, while Tsvetanova and Stefanova outlined common cyber threats faced by financial organizations.

Boitan classified cyberattacks into four main categories, highlighting that attacks on critical financial services can undermine the stability of the entire financial system. Nobles pointed out vulnerabilities such as sophisticated cyberattacks, social engineering, credit card fraud, and online banking scams. Jakovljević identified mobile applications and web portals as significant sources of cyber risk in banking.

The literature also categorizes cyber threats based on their nature and origin. Targeted attacks focus on specific organizations and tend to be carried out by skilled cybercriminals, whereas non-targeted attacks aim at any vulnerable system and are often less sophisticated. Additionally, threats can be external—originating from outside hackers—or internal, coming from employees or contractors abusing authorized access.

Common cyber threats in banking include malware, phishing, distributed denial-of-service (DDoS) attacks, and insider threats. Malware is malicious software designed to steal sensitive information or disrupt operations. Phishing uses deceptive emails or websites to trick users into revealing confidential data. DDoS attacks overwhelm systems with traffic to disrupt services, while insider threats involve misuse of access privileges by trusted individuals.

To address these challenges, various countermeasures have been proposed. Dubois and Tatar emphasized the importance of cybersecurity training and simulation environments to prepare staff for attacks. Al-Alawi and Al-Bassam highlighted raising cybersecurity awareness among banking employees as a key defense.

Moreover, frameworks have been developed to better assess cyber risks, incorporating factors like threat actors, vulnerabilities, safeguards, and consequences.

Strategic management tools such as the Balanced Scorecard have been suggested to help banks mitigate cyber fraud by considering non-financial factors alongside traditional metrics. Research also points to gaps in crisis management, particularly in how financial sectors collect and analyze information about cyber threats. Studies on banking Trojans and other malware have improved understanding of attack stages, aiding in detection and mitigation.

Finally, regulators and central banks have begun adopting risk-based approaches to strengthen cybersecurity frameworks across the financial industry. Despite these advances, the dynamic nature of cyber threats means ongoing research is essential, especially to refine threat classifications and develop effective, innovative countermeasures.

CHAPTER - 3
SYSTEM METHODOLOGY

3.1 Research Design and Framework development

This section outlines the research design adopted to construct a robust framework for **Cyber Threat Classification and Countermeasures** specific to the Banking and Financial Sector. The methodology is inspired by prior studies and follows a structured, iterative approach aimed at developing a practical, adaptive, and comprehensive framework. The development process consists of several sequential steps: identifying key components, defining classification criteria, integrating threat intelligence, constructing taxonomy, determining the level of granularity, and assigning threat severity levels or risk scores. Each of these stages is informed by findings from an extensive literature review and industry best practices.

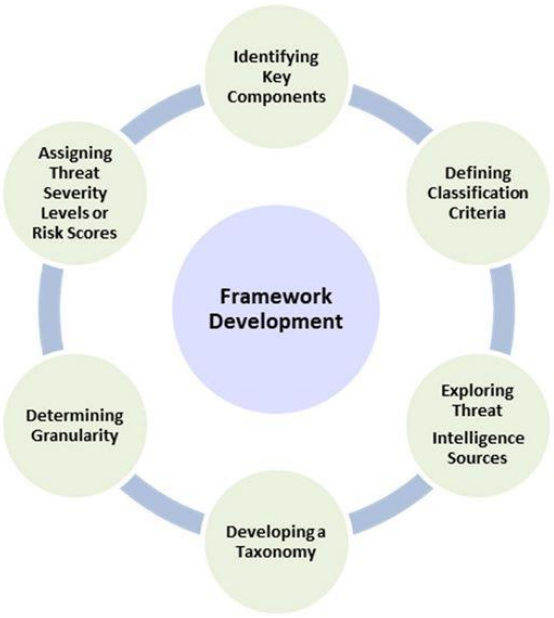

Figure 3.1 Framework Development

A. Identifying Key Components

The first step involves determining the essential components that underpin the framework. This is achieved by reviewing existing cybersecurity models, industry guidelines, and academic research. Key components include threat categories, attack vectors, vulnerability types, impact parameters, and associated mitigation strategies.

B. Defining Classification Criteria

After identifying the components, classification criteria are established. These criteria are intended to be specific and measurable, enabling structured categorization of threats based on characteristics such as type, severity, and relevance. They form the foundation for consistent threat labeling aligned with the research objectives.

C. Exploring Threat Intelligence Sources

To ensure the framework remains grounded in real-world contexts, diverse threat intelligence sources are examined. These include commercial security feeds, government alerts, industry-specific Information Sharing and Analysis Centers (ISACs), and open-source databases. Incorporating these sources helps capture emerging threats and indicators of compromise relevant to the financial sector.

D. Developing a Taxonomy

This step involves organizing identified threats into a structured taxonomy, comprising categories, subcategories, and associated attributes. The taxonomy is designed to be flexible, supporting the addition of new threat types and evolving attack vectors while preserving consistency in classification.

E. Determining Granularity

Granularity refers to the level of detail with which threats are categorized. It is carefully calibrated to balance complexity with practicality, considering the resource constraints, technical maturity, and specific needs of banking and financial institutions.

F. Assigning Threat Severity Levels or Risk Scores

To support prioritization of threats, the framework includes a mechanism to assign severity levels or risk scores. This is based on parameters such as potential impact, likelihood of occurrence, and alignment with risk management frameworks. A transparent, standardized scoring system is employed to ensure objective and actionable outputs. The entire framework development is iterative, allowing for ongoing refinement in response to new threat intelligence, real-world incidents, and

stakeholder feedback. This adaptability ensures the framework remains effective in the ever-evolving cyber threat landscape faced by the banking and financial sector.

3.2 Cyber threats Framework

Cyber threats pose serious challenges to the banking and financial sector due to the sensitive nature of the data and the criticality of uninterrupted operations. This framework classifies cyber threats into four aspects: **impact**, **nature**, **characteristics**, and **classification criteria**.

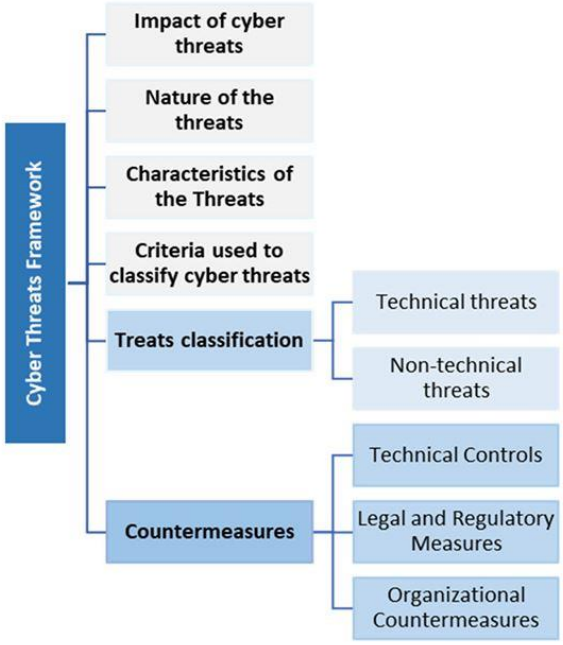

Figure 3.2 Cyber threats Framework

A. Impact of Cyber Threats

Cyber threats pose serious risks to the banking and financial sectors due to the sensitive and confidential nature of financial data. These threats can significantly compromise the stability, security, and integrity of institutions, making it essential to understand their potential implications. This section presents a structured analysis of the various dimensions of cyber threats, offering a comprehensive framework that classifies their impacts into distinct categories. The classification was derived from real-world incidents, expert opinions, and industry reports. It includes:

- **Financial Impact**: Direct monetary losses from fraud, theft, or ransomware.

- **Operational Impact**: Disruption of core banking operations and critical infrastructure.
- **Reputational Impact**: Loss of customer trust and damage to brand credibility.
- **Regulatory Impact**: Challenges in maintaining compliance and dealing with regulatory penalties.
- **Legal Impact**: Potential lawsuits, legal actions, and liabilities stemming from data breaches or compliance failures.

Both immediate (e.g., infrastructure disruption) and long-term (e.g., reputational damage) consequences were considered in this evaluation. By understanding these impacts, institutions can better allocate resources, prioritize mitigation strategies, and enhance their incident response and risk management frameworks.

B. Nature of Cyber Threats

Understanding the nature and characteristics of cyber threats is essential for developing effective detection, prevention, and response strategies. These threats are multifaceted, targeting sensitive financial data and exploiting vulnerabilities in systems and human behavior.

The nature of cyber threats is defined by several key dimensions:

- **Adversarial Intent**: Threat actors deliberately target financial institutions for financial gain.
- **Rapid Evolution**: Cyber tactics and tools change frequently, making defense more challenging.
- **Covert Operations**: Threats often go undetected for extended periods, increasing potential damage.
- **Sector-Wide Targeting**: Threats span across various financial services and infrastructures.
- **Motivations**: Attacks are driven by financial, ideological, or political motives.

C. Characteristics of Cyber Threats

The character of cyber threats refers to the attributes, motivations, and goals of threat actors targeting the banking and financial sector. Understanding these traits is vital for anticipating attacker behavior and enhancing response strategies.

Key characteristics include:

- **Insider Involvement**: Internal actors pose a major threat to sensitive data and transactions.
- **Multi-Vector Attacks**: Cybercriminals use multiple methods to maximize impact and evade detection.
- **Sophistication**: Advanced tools and techniques are often used to penetrate defenses.
- **Use of Legitimate Tools**: Attackers may exploit trusted software to avoid security triggers.
- **Adaptability and Persistence**: Threat actors continuously evolve and maintain prolonged efforts.
- **Coordination and Organization**: Many attacks are executed by well-structured, collaborative groups.
- **Global Reach and Targeting**: Cyber threats are geographically distributed and target various assets.
- **Motivations**: Ranging from financial gain to political objectives.

These dimensions provide insights into the complexity of cyber threats, helping institutions to build stronger, more targeted cyber security measures.

D. Criteria used to classify cyber threats

To manage cyber threats effectively, it is essential to classify them using multiple criteria. Threat Impact and Threat Severity are top priorities, as they indicate the potential damage and seriousness of an attack. Other key factors include Attack Type, Threat Vector, Threat Origin, Threat Actor, and Motivation, each contributing to a deeper understanding of how, where, and why an attack occurs.Technical aspects such as Vulnerability Type, Targeted Assets, and Attack Complexity help identify exploited weaknesses. Detection and Response Capabilities reflect an organization’s

ability to react to threats. Additional factors like Frequency, Geographical Distribution, and Emerging Technologies support long-term threat analysis and preparedness.

This comprehensive classification enables improved threat assessment, prioritization, and cybersecurity planning. The study categorizes these criteria into different dimensions and ranks them based on their severity, importance, and potential impact.

Dimension	Description	Criteria under dimension
Threat Characteristics Dimension	This dimension captures the nature of the threat itself	Attack Type [44], Threat Vector [41], Threat Origin [42], Vulnerability Type [38], Attack Complexity [32][44], Attack Surface [32], Threat Lifecycle [45], Tools and Techniques [16][41], Frequency [41]
Threat Actor Dimension	This dimension focuses on the entity or entities responsible for the threat	Threat Actor [43], Threat Motivation [43], Geographical Distribution [42]
Impact Dimension	This dimension assesses the potential or actual consequences of a threat	Threat Impact [33][44], Threat Severity [33], Targeted Assets [43], Attack Objective [30]
Defense Dimension	This dimension concerns the capabilities and actions of the target to detect, respond, and prevent threats	Detection and Response Capabilities [31], Countermeasure Effectiveness [30], Indicators of Compromise (IoCs) [46]
Future Trends Dimension	This dimension anticipates the evolution of cyber threats	Emerging Trends and Technologies [47]

Figure 3.3 Dimensions of Cyber threats criteria

E. Threat Classification

This section presents a comprehensive classification of threats faced by the Banking and Financial Sector, divided into two main categories: **technical threats** and **non-technical threats**. This framework enables a systematic understanding of the diverse threat landscape, improving threat analysis, incident response, and risk management.

Technical threats exploit system vulnerabilities using tools and techniques such as network breaches, malware, DDoS attacks, and supply chain attacks.

Advanced Persistent Threats (APTs) are the most severe, involving long-term, sophisticated attacks aimed at stealing sensitive data. Other notable technical threats include phishing, mobile banking threats, IoT vulnerabilities, zero-day exploits, credential stuffing, and cloud security risks.

Non-technical threats rely on human factors, including social engineering, insider threats, identity theft, and business email compromise. These are often harder to mitigate due to their reliance on behavior and organizational policies. Physical security breaches, third-party risks, employee negligence, legal and regulatory challenges, and shadow IT also contribute to this category.

The classification highlights the severity and impact of each threat type, helping the sector prioritize defenses and response strategies.

CHAPTER - 4
RESULTS AND INFERENCES

From the study, it's clear that protecting banks and financial institutions from cyber threats requires a mix of different approaches working together. On the technical side, tools like encryption are the most effective because they keep sensitive data safe from unauthorized access. Other important technical measures include multi-factor authentication, network segmentation, firewalls, and regular updates to fix security gaps. These tools help create strong barriers against cyber-attacks, but their success depends on how well they fit the specific risks an organization faces. Legal and regulatory measures also play a big role. Laws and regulations around data protection and mandatory breach reporting help set clear rules that organizations must follow, which encourages better security practices. Frameworks and international cooperation add another layer of support by sharing standards and helping to reduce financial and reputational damage from attacks.

Equally important are the organizational steps that institutions take. Building a culture where everyone understands the importance of cyber security is key. This includes training employees regularly, having clear policies, planning for how to respond to incidents, and managing risks continuously. Assigning dedicated cyber security roles, testing systems regularly, and preparing for business disruptions all contribute to stronger defences. Overall, the takeaway is that there's no single fix for cyber security. Instead, banks and financial services need a well-rounded strategy that combines technical tools, legal compliance, and organizational efforts. When these are tailored to an organization's unique needs and risks, they work best to keep cyber threats at bay and protect critical information.

CHAPTER - 5
CONCLUSION

In today's fast-paced digital world, banks and financial institutions face a growing wave of cyber threats. To stay safe, they need more than just one type of defence — a mix of technical tools, clear rules and regulations, and strong organizational practices all working together is the best way forward. This combined approach not only helps stop attacks but also creates a security-minded culture that makes the whole organization stronger and more ready to handle problems. This study looked closely at the kinds of cyber threats that target banks and the different ways to reduce their risks. As technology keeps changing, new challenges keep popping up, so banks need to stay alert and constantly improve their defences. We found that technical protections, legal rules, and good company practices all play important roles in keeping data safe, building customer trust, and avoiding costly damages.

Working together — from leadership to every employee — and managing risks thoughtfully is key to protecting the financial sector from cyber-attacks. The ideas and strategies shared here can help banks and policymakers create better security plans that stay ahead of cyber criminals. In short, this research offers a clear roadmap for understanding cyber threats and taking effective action. By following these insights, financial institutions can build stronger defences and be ready for whatever cyber challenges come next.

REFERENCES

[1] A. Raghavan and L. Parthiban, ‘‘The effect of cybercrime on a bank’s finances,’’ Int. J. Current Res. Academic Rev., vol. 2, no. 2, pp. 173–178, 2014.

[2] M. Hanif, ‘‘Differences and similarities in Islamic and conventional banking,’’ Int. J. Bus. Social Sci., vol. 2, no. 2, pp. 1–25, Apr. 2014.

[3] D.-Y. Kao, ‘‘Cybercrime countermeasure of insider threat investigation,’’ in Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT), Feb. 2019, pp. 413–418.

[4] M.Kartiwi, T.Arundina, M.A.Omar, and T.S.Gunawan,‘‘S-Rater:Data mining application in Islamic financial sector,’’ in Proc. 5th Int. Conf. Inf. Commun. Technol. Muslim World (ICT4M), Nov. 2014, pp. 1–5.

[5] Z. Ghasemi, M. A. Kermani, and T. Allahviranloo, ‘‘Exploring the main effect of e-Banking on the banking industry concentration degree on predicting the future of the banking industry: A case study,’’ Adv. Fuzzy Syst., vol. 2021, Aug. 2021, Art. no. 8856990.

[6] GuardRails. (Jul. 22, 2022). The Top 10 Cybersecurity Threats to Digital Banking and how to Guard Against Them. Accessed: May 16, 2023.

[7] B. Sheehan, F. Murphy, A. N. Kia, and R. Kiely, ‘‘A quantitative bow-tie cyber risk classification and assessment framework,’’ J. Risk Res., vol. 24, no. 12, pp. 1619–1638, 2021.

[8] G.J.W.Kathrine, P.M.Praise, A.A.Rose, and E.C.Kalaivani,‘‘Variants of phishing attacks and their detection techniques,’’ in Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI), Apr. 2019, pp. 255–259.

[9] O. Shulha, I. Yanenkova, M. Kuzub, I. Muda, and V. Nazarenko, ‘‘Banking information resource cyber security system modeling,’’J.OpenInnov., Technol., Market, Complex., vol. 8, no. 2, p. 80, Jun. 2022.

[10] A.Bani-Hani, M.Majdalweieh, and A.AlShamsi,‘‘Online authentication methods used in banks and attacks against these methods,’’Proc.Comput. Sci., vol. 151, pp. 1052–1059, Jan. 2019.