International Journal of Economics and Business Management Research
ISSN: 3107-9423 | Volume 2 Issue 2, 174-183, April-June 2026
DOI: https://doi.org/10.64137/31079423/IJEBMR-V2I2P121

Received: 01/05/2026 Revised: 28/05/2026 Accepted: 02/06/2026 Published: 04/06/2026

Original Article

A Study on Cybersecurity Risks in Financial Institutions

[1]S. SATHISH KUMAR, [2]M. MUKESH KUMAR
[1]Assistant Professor, Department of Management Studies, E.G.S. Pillay Engineering College, Tamil Nadu, India.
[2]Student, Department of Management Studies, E.G.S. Pillay Engineering College, Tamil Nadu, India.

ABSTRACT: *The rapid growth of digital banking and online financial services has increased the importance of cybersecurity management in financial institutions. Financial organizations are highly dependent on digital technologies for banking operations, online transactions, mobile banking, and customer data management. This technological advancement has also increased cyber threats such as phishing attacks, malware attacks, ransomware, hacking, identity theft, and data breaches. These cyber risks affect customer trust, financial stability, operational efficiency, and organizational reputation. The main objective of this study is to analyze the importance of cybersecurity management in financial institutions and examine various cyber threats, security challenges, and preventive measures used to protect digital financial systems. The study also focuses on emerging cybersecurity technologies such as Artificial Intelligence, Machine Learning, Blockchain Technology, Cloud Security, and Biometric Authentication used for improving digital security management. The research is based on secondary data collected from books, journals, websites, research articles, banking reports, and cybersecurity publications. Percentage analysis, charts, graphs, and interpretation methods are used to analyze cybersecurity trends and digital security practices in financial institutions. The findings of the study reveal that effective cybersecurity management plays a significant role in protecting confidential customer information, ensuring secure digital transactions, reducing cyber risks, and maintaining business continuity. The study concludes that financial institutions must continuously strengthen cybersecurity infrastructure, improve employee and customer awareness, and adopt advanced security technologies to manage evolving cyber threats and maintain secure financial operations in the modern digital environment.*

KEYWORDS: *Cybersecurity, Financial Institutions, Digital Banking, Cyber Threats, Data Protection, Information Security, Cyber Risk Management.*

1. INTRODUCTION

As the financial industry embraces a digital transformation induced through rapid advances in technology like digital banking, internet banking, mobile banking, cloud computing, and online financial services, cybersecurity is increasingly one of its top priorities. Financial institutions are using digital technologies increasingly to carry out many of their banking operations, preserving customer logs, processing transactions online & serving the financial services proficiently. Continuous emergence of digital platforms has directly improved customer convenience as well as transaction speed and operational efficiency. But the rapid proliferation of digital systems also presents huge cybersecurity challenges and opportunities for financial institutions.

Financial institutions process high-value and sensitive customer data that consists of bank account details, transaction history, passwords, credit card numbers & expiration dates, debit card details, and digital payment information. Due to the criticality of this information, financial institutions have evolved into a field day for hackers and online persuasion. Cyberattacks like phishing attacks, Malware infections, Ransomware attacks, Hacking, Identity thefts, Data breaches, and cyber fraud pose a substantial risk to organizations both financially as well as operationally. These cyber threats not only impact the performance of an organization, but they also lead to the loss of customer trust and reputation damage to the organization's reputation.

The world of banking and Finance has changed massively due to the rapid rise in digital technologies and internet-based financial services. In recent years, the convenience and accessibility of online banking and digital payment systems have encouraged customers to rely on such channels for their financial transactions. In the last few years, there has been rapid growth of services like mobile banking applications, internet fund transfer & UPI transactions, digital wallets, and online payment gateways. To earn customer satisfaction and remain competitive in the financial market, financial institutions constantly need to release new digital services.

While some benefits of banking are enhanced through digital use, it also leads to an increased possibility of cybersecurity vulnerabilities and exposure to digital risk. With robust, evolving hacking techniques and cyberattack methods designed to leverage weaknesses in banking systems or digital networks, cybercriminals are constantly inventing new ways to break existing technologies. Cyberattacks may result in financial fraud, corporate espionage, operational disruption, and regulatory

violations for these companies. Hence, proactive and robust practices of cybersecurity management are crucial for securing the digital financial ecosystem with secure online transactions.

Cybersecurity is the process of protecting our computer systems, digital networks, software applications, and confidential information from unauthorized access, cyber threats, and online attacks. A good security system for business or cybersecurity management contains many features like encryption technologies, firewall protection, fraud detection systems, multi-factor authentication below both the server & client-side, and biometric authentication. This also allows financial institutions to better manage cyber-risks and improve digital security.

1.1. IMPORTANCE OF CYBERSECURITY IN FINANCIAL INSTITUTIONS

Cybersecurity is one of the most important functions for financial institutions since modern banks rely entirely on digital technologies and internet-based financial services. Every day, financial institutions handle enormous amounts of private customer data, transaction logs, online payment systems, and digital banking functionality. With the surge in internet banking, mobile banking, digital wallets, UPI transactions, and cloud-based financial services, demand for robust cybersecurity systems has grown significantly within organisations. The growth of digitalisation has seen many financial institutions increasingly targeted by cybercriminals and online fraud. As a result, proper cybersecurity management is now vital to the security of financial systems, consumer identities, and digital banking infrastructure.

Customer confidentiality is one reason why cybersecurity is very relevant in financial institutions. Banks and financial organizations save the data that include account information, passwords, ATM PIN, debit card number and CVV code, credit card number, CVV code, and transaction history, in addition to the personal identification records. This information is constantly under siege by cybercriminals via phishing attacks, malware attacks, ransomware attacks, hacking, and identity theft operations. This, in turn, safeguards customer data from unauthorized access and cyber fraud due to the presence of strong cybersecurity systems within financial institutions.

Secondly, cybersecurity is important for secure transactions and online banking. Customers these days want safe, sound, and secure digital banking platforms whenever they are executing their financial activity through internet banking and mobile banking applications. To achieve secure, safe, and seamless transactions electronically, financial institutions implement advanced identity verification technologies such as encryption systems, firewall protection for broadband connectivity or network fraud monitoring tools (FMS), and emerging security software applications like intrusion detection systems (IDS), Multi-Factor Authentication Systems (MFA), and biometric verification systems for online banking safety. Such security measures minimize cyber risk and bolster customer confidence in digital financial services.

1.2. GROWTH OF DIGITAL BANKING

In recent years, the banking and financial sector has seen a significant transformation in the form of digital banking. As financial institutions begin to operate differently in the way that they provide banking services to customers with advances in information technologies, internet services, smartphones, and digital payment systems. Internet banking, mobile banking apps, digital wallets, online fund transfer options, and cashless payment systems are how many people now perceive or know about the concept of traditional banking. The traditional visual of customers standing in line for info at a Bank tone must be completely erased. Now open, Customers will prefer Digital Banking services to provide all the convenience & speed with millisecond access, along with service efficiency without coming down directly to the Bank branches for growing & completing their financial transactions!!

Digital banking is a form of e-banking that enables the customer to access banking products and services anytime, anywhere, from smartphones, computers, or other internet-enabled devices. Digital banking provides custom catalog options for making money transfers, utility payments, balance inquiries, loan applications, mobile recharges, and online shopping transactions to customers. It has also led to enhanced customer satisfaction within financial institutions and lower transaction processing time. With the incorporation of digital technologies, it has become easier for financial organizations to streamline their operational efficiencies and eliminate manual banking activities.

1.3. EMPLOYEE ROLES IN CYBERSECURITY

Employees play an important role in maintaining cybersecurity within financial institutions. Human errors, lack of awareness, weak passwords, and negligence often create cybersecurity vulnerabilities.

Financial institutions conduct employee training programs and awareness sessions to educate employees about phishing attacks, password protection, safe internet practices, and cybersecurity policies.

1.4. CUSTOMER ROLES IN CYBERSECURITY

Customers also play an important role in cybersecurity management by following safe digital banking practices. Customers should use strong passwords, avoid sharing OTPs, and verify official banking websites before performing online transactions.

Customer awareness helps reduce cyber fraud, identity theft, and unauthorized banking activities in digital financial systems.

1.5. CYBERSECURITY AWARENESS PROGRAMS

Cybersecurity awareness programs improve digital security knowledge among employees and customers. Financial institutions organize workshops, training sessions, and awareness campaigns to educate individuals about cyber threats and safe online practices.

These programs help reduce cybersecurity risks and strengthen organizational cybersecurity management practices.

1.6. BENEFITS OF CYBERSECURITY

Cybersecurity provides several benefits to financial institutions by protecting customer information, reducing cyber risks, and ensuring secure digital transactions.

Strong cybersecurity systems improve customer trust, organizational reputation, operational stability, and business continuity in financial institutions.

2. REVIEW OF LITERATURE

- William Stallings (2018): explained important cybersecurity principles, network security threats, and protection mechanisms used in modern organizations. The study focused on methods for protecting digital systems and confidential information from cyberattacks.
- Charles P. Pfleeger (2015): discussed system vulnerabilities, cyber risks, and security control mechanisms in organizations. The study highlighted the importance of maintaining secure information systems and protecting organizational data.
- Shari Lawrence Pfleeger (2015): focused on cybersecurity risk management and access control systems. The study explained the role of security policies and risk assessment techniques in improving cybersecurity management.
- Nina Godbole (2011): studied cybercrimes, online fraud activities, and digital security practices. The research emphasized the importance of cybersecurity awareness and preventive measures in reducing cyber risks.
- Sunit Belapure (2011): explained computer forensics, cyber laws, and cybersecurity investigation methods. The study focused on legal frameworks and digital evidence management in cybercrime investigations.
- Joseph Migga Kizza (2020): discussed network security management and cyber defense strategies. The study highlighted various methods used to protect organizational networks from cyber threats and unauthorized access.
- Bruce Schneier (2015): emphasized privacy risks, data protection, and digital security challenges in modern organizations. The study explained the importance of maintaining customer privacy and securing confidential information.
- Ross J. Anderson (2020): explained security engineering methods and cybersecurity management techniques. The study focused on system security design and secure communication systems in organizations.
- Mark Rhodes-Ousley (2013): focused on enterprise security management and organizational cybersecurity practices. The study highlighted the importance of strategic security planning and digital risk management.
- Jason Andress (2014): explained information security concepts, cybersecurity basics, and best security practices. The study focused on protecting digital systems and improving cybersecurity awareness.
- Michael E. Whitman (2023): studied organizational security principles and information security management systems. The study emphasized the importance of cybersecurity policies and digital security governance.
- Herbert J. Mattord **(**2018): explained cybersecurity frameworks, security policies, and organizational security management practices. The study focused on improving cybersecurity planning and risk management activities.
- Kevin Mitnick (2017): emphasized digital privacy, cybersecurity awareness, and online safety practices. The study highlighted how social engineering and human errors contribute to cybersecurity risks.
- Gary McGraw (2006): focused on software security risks and secure software development practices. The study explained methods for identifying software vulnerabilities and improving application security.
- Jonathan Katz (2019): discussed modern cryptographic techniques and secure communication systems. The study focused on encryption technologies and methods used for protecting confidential digital information.

3. OBJECTIVE OF THE STUDY

- To identify the major types of cybersecurity threats affecting financial institutions.
- To examine the causes and contributing factors of cybersecurity breaches in financial institutions.
- To assess the impact of cyberattacks on financial performance, reputation, and customer trust.
- To evaluate the effectiveness of existing cybersecurity risk management practices.
- To analyze the level of employee awareness and training regarding cybersecurity issues.

4. RESEARCH METHODOLOGY

4.1. RESEARCH DESIGN

Research design is the blueprint or framework used to conduct the study systematically. For the present study, a **d**escriptive research design has been adopted. Descriptive research helps in describing the characteristics, patterns, and current conditions related to cybersecurity risks in financial institutions.

The study aims to analyze existing cybersecurity threats, digital risks, and protection mechanisms followed in financial institutions.

4.2. NATURE OF STUDY

The study is analytical and descriptive in nature. It mainly focuses on analyzing existing information related to cybersecurity risks and understanding their relevance in the financial sector.

The research examines common cybersecurity issues such as phishing attacks, malware attacks, ransomware, data breaches, insider threats, and unauthorized access.

4.3. SOURCE OF DATA

The study is based mainly on **secondary data**.

4.4. SECONDARY DATA

Secondary data refers to information that has already been collected and published by other sources. For this study, secondary data have been collected from:

- Books related to cybersecurity and information security
- Journals and research articles
- Company annual reports
- Banking sector reports
- Websites and online publications
- Government reports
- News articles and case studies

Secondary data helps in understanding industry trends, security challenges, and risk management practices followed by financial institutions.

4.5. SAMPLING TECHNIQUE

As the study is based on secondary data, sampling is not directly applicable in the traditional sense. However, relevant data sources, reports, journals, and financial institution records were selected purposively based on the study objectives.

A purposive sampling technique was used to select information sources that are directly related to cybersecurity and financial institutions.

4.6. AREA OF STUDY

The study focuses on cybersecurity risks affecting financial institutions, including:

- Commercial banks
- Private banks
- Public sector banks
- Digital payment service providers
- Financial technology companies

Special emphasis is given to digital banking systems and online transaction security.

4.7. PERIOD OF STUDY

The study covers data and information collected from recent years to understand the evolving cybersecurity landscape in financial institutions.
The study period includes recent trends, cybersecurity incidents, and security developments in the banking and financial sector.
"The study covers the period from 2020 to 2025."

4.8. TOOLS USED FOR ANALYSIS

The collected data is analyzed using simple analytical methods such as:
The collected data for the present study have been analyzed using simple statistical tools to interpret the findings effectively. The major analytical tools used in this study are percentage analysis, comparative analysis, descriptive interpretation, and graphical representation

- Percentage analysis
- Comparative analysis
- Descriptive interpretation
- Graphical representation

These tools help in understanding cybersecurity trends and risks more effectively.

4.9. RESEARCH VARIABLES

The major variables considered in the study include:

- Cybersecurity threats
- Data breaches
- Fraud risks
- Digital transaction security
- Customer data protection
- Security frameworks

These variables are relevant to analyzing cybersecurity risks in financial institutions.

4.10. LIMITATIONS OF RESEARCH METHODOLOGY

The study has certain limitations:

- The study is based only on secondary data
- Availability of updated cybersecurity data may be limited
- Findings depend on published information sources
- Rapid technological changes may influence results

4.11. PERCENTAGE ANALYSIS

Percentage analysis is one of the statistical tools used in this study to analyze and present secondary data in a simple and meaningful manner. It helps in understanding the relative proportion of various cybersecurity risks, impacts, security measures, and emerging technologies identified from published reports, research articles, journals, and other secondary sources. The percentage values are used to facilitate comparison and interpretation of cybersecurity trends in financial institutions.

Formula:
Percentage = (Particular Value / Total Value) × 100

Where:

- Particular Value = Value of a specific category selected for analysis
- Total Value = Total value considered for the study.

5. DATA ANALYSIS AND INTERPRETATION

Data analysis is the process of examining and interpreting collected data to derive meaningful conclusions. The present study is based on secondary data collected from books, journals, annual reports, websites, research articles, and financial institution reports related to cybersecurity risks in financial institutions.

The analysis focuses on identifying major cybersecurity risks, their impact on financial institutions, security measures adopted, and emerging technologies used to reduce cyber threats.

FIGURE 1 Types of Cybersecurity Risks in Financial Institutions

	Percentage
Phishing Attacks	30%
Malware Attacks	20%
Data Breaches	18%
Ransomware	12%
Insider Threats	10%
Identity Theft	10%
Total	**100%**

Formula

Percentage = (Particular value / Total Value) × 100

Interpretation

The above table indicates that phishing attacks represent the highest cybersecurity risk with 30%, followed by malware attacks with 20% and data breaches with 18%. This shows that phishing remains a major threat in financial institutions.

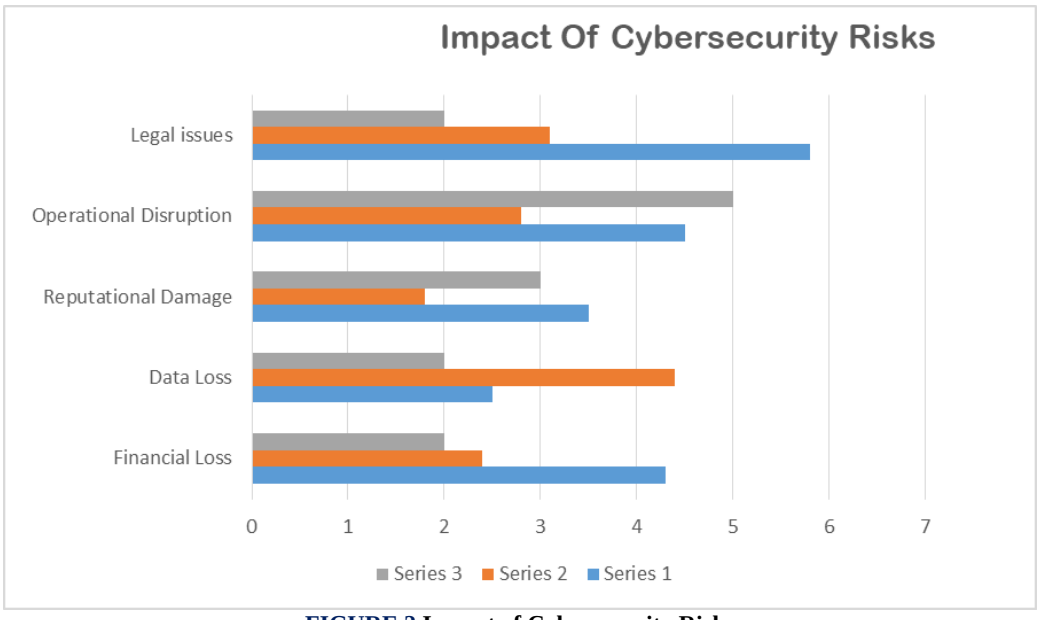

FIGURE 2 Impact of Cybersecurity Risks

Financial Loss	35%
Data Loss	25%
Reputational Damage	20%
Operational Disruption	12%
Legal Issues	8%
Total	**100%**

Formula

Percentage = (Particular value / Total Value) × 100

Interpretation

The above table shows that financial loss is the major impact of cybersecurity risks, with 35%, followed by data loss at 25%. This indicates that cyberattacks significantly affect financial institutions both economically and operationally.

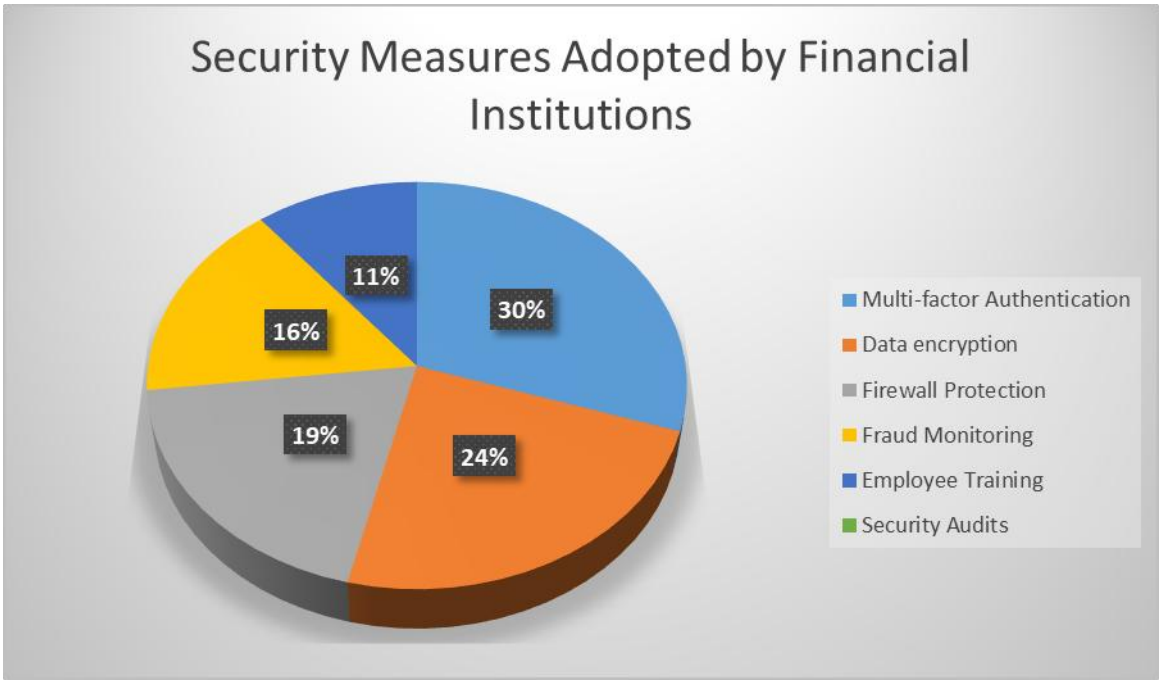

FIGURE 3 Security Measures Adopted by Financial Institutions

	Percentage
Multi-Factor Authentication	28%
Data Encryption	22%
Firewall Protection	18%
Fraud Monitoring	15%
Employee Training	10%
Security Audits	7%
Total	**100%**

Formula

Percentage = (Particular value / Total Value) × 100

Interpretation

The table shows that multi-factor authentication is the most widely used cybersecurity measure, with 28%, followed by data encryption with 22%. This indicates the importance of authentication and data protection in financial institutions.

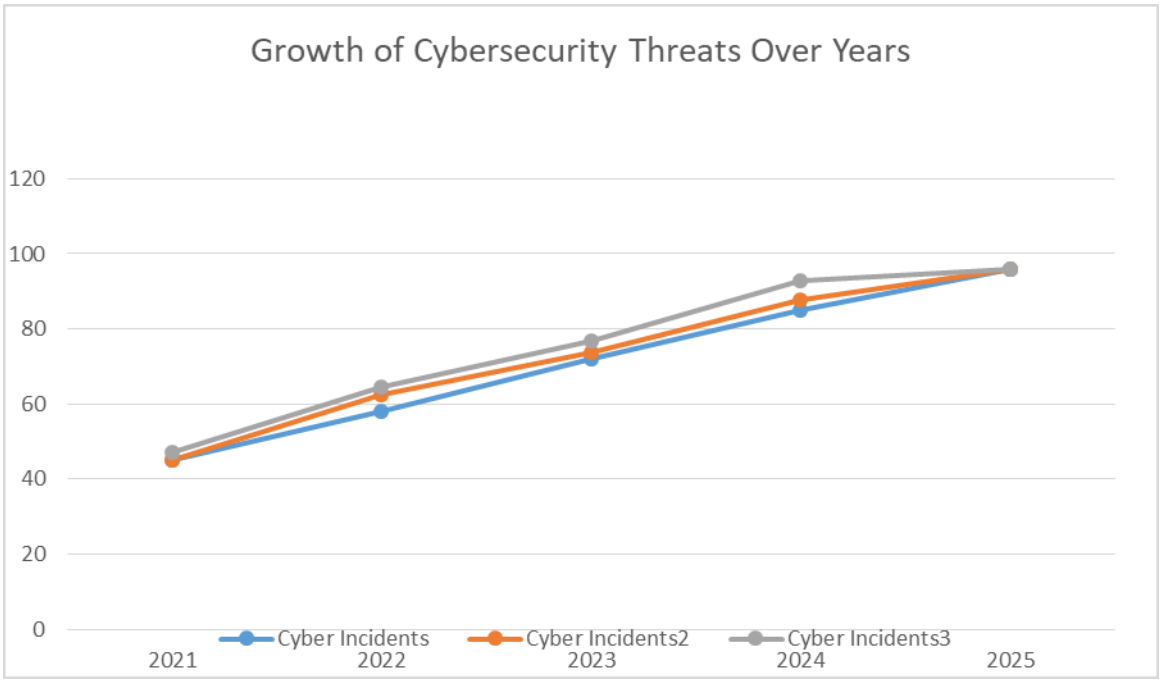

FIGURE 4 Growth of Cybersecurity Threats over the Years

2021	45
2022	58
2023	72
2024	85
2025	96

Formula

Growth Rate = (Current Year - Previous Year)/ previous year × 100

Interpretation

The above table indicates a steady increase in cybersecurity incidents in financial institutions from 45 incidents in 2021 to 96 incidents in 2025. This reflects the growing cybersecurity challenges in the financial sector.

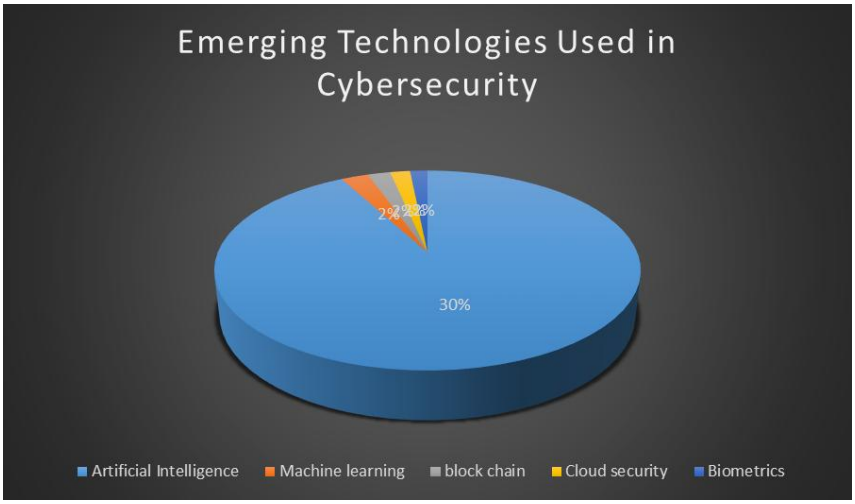

FIGURE 5 Emerging Technologies Used in Cybersecurity

	Percentage
Artificial Intelligence	30%
Machine Learning	22%
Block chain	18%
Cloud Security	16%
Biometrics	14%
Total	**100%**

Formula

Percentage = (Particular value / Total Value) × 100

Interpretation

The table shows that Artificial Intelligence is the most widely adopted emerging cybersecurity technology, with 30%, followed by Machine Learning with 22%.

6. RESULTS AND INTERPRETATION

The analysis of cybersecurity risks in financial institutions shows that phishing attacks are the most common cybersecurity threat, with 30%, followed by malware attacks at 20% and data breaches at 18%. This indicates that cybercriminals mainly target customers and employees through fraudulent emails, fake websites, and malicious software to gain unauthorized access to financial information. The increasing use of digital banking and online transactions has further increased the risk of phishing and malware attacks in financial institutions.

Cybersecurity risks also severely impact financial institutions, the study says. Financial Loss acts on more than a third, doing 35%, followed by data loss at 25%, and reputational damage falls alone at 20%. This goes to show that cyberattacks do not just harm organizational finances but also cause operational disruption and litigation, which also undermine the resilience and performance of financial institutions.

Analysis: Data encryption is the second most widely used security measure among financial institutions at 22%, while multi-factor authentication is first with 28%, followed by firewall protection (18%). The aforementioned statistics portray the increasing relevance of authentication systems and data protection technologies in the mitigation of cyberattacks to enable safe banking services online.

The research also depicts an everlasting rise in threats over the years. The results show that the number of cybersecurity incidents rose from 45 cases in 2021 to 96 cases in the financial sector by FY25, which is quite fast. Rapid adoption of digital banking systems, online transactions, and enhancements in internet-based financial services have also led to a significant increase in cybersecurity incidents.

The study of the emerging technologies used in cybersecurity shows that 30% of organizations have adopted Artificial Intelligence, 22% Machine Learning, and 18% Block chain Technology. These technologies are valuable to financial institutions, improving threat detection, monitoring credit card fraud, securing transactions, and cyber security management practices. This trend highlights how digital security innovation is playing an important role in protecting financial systems from constantly evolving cyber threats through advanced technologies.

In sum, the system-wide findings show that, with advances in technology and ICT-financial services, cybersecurity-related risks for financial institutions are significantly higher. You should have effective cybersecurity management, advanced security technologies, employee awareness programs, and advanced security measures to minimize cyber risks and implement secure digital banking.

7. CONCLUSION

The study concluded that the surge of modern banking, e-commerce, mobile banking, and internet-based financial services has made cybersecurity risk one of the leading challenges facing Financial Institutions. Digital technologies are being used more by financial institutions to carry out their banking operations, provide customer services, and process transactions. The digital transformation does enhance operational efficiency and customer convenience, but at the same time, it exposes organizations to cyber vulnerabilities and cybercrimes. Cyber threats like phishing, malware, ransomware, identity theft, insider threats, and data breaches pose severe financial, operational, and reputational risks to financial institutions.

The study results show that phishing, malware, and data breaches are the three most impactful cyber threats facing financial institutions, with phishing being ranked the top threat. Cybersecurity incidents result in financial losses, operational

disruptions, legal liabilities, reputational harm, and diminished customer trust. These challenges have emphasized the crucial need for efficient management practises to safeguard digital financial systems and sensitive customer data.

Moreover, the study finds that financial institutions are implementing multiple security measures,, including multi-factor authentication and data encryption, as well as data loss prevention techniques such as firewall protection, fraud monitoring systems, and employee cyber awareness programs, to mitigate the risks of cyber incidents and improve digital security management. Cybersecurity solutions can be strengthened further with the hot new emerging trusted technologies like: Artificial Intelligence & Machine Learning, Blockchain Technology used As A Tool For Cyber Security, Cloud Security Protection from Cyber Attacks, and Biometric Authentication in the financial industry, placed in a few of the financial institutions!

Here are the top two recommendations for you: Make your employees aware of them on one side, and educate customers on the other. Cybersecurity vulnerabilities in organizations are often compounded by human errors, ignorance, weak passwords, and negligence. Hence, financial institutions should be holding continuous cybersecurity awareness programs, employee training sessions, workshops, and customer education campaigns to enhance their security understanding and secure digital banking behavior.

The study also finds that cybersecurity threats are rapidly growing with the technological advancements and increasing reliance on digital financial services. It therefore requires controlling different levels of cyber threats, such as improving cybersecurity infrastructure, implementing advanced security technologies, upgrading cybersecurity policies, and performing routine security monitoring activities by the financial institution.

In conclusion, effective cybersecurity management of sensitive data in financial institutions helps safeguard the privacy of confidential customer information and secure online transactions, maintain business continuity by preventing downtime and operational concerns, strengthen a firm's reputation or brand image, leading to increased customers' trust and confidence in their ability to run such services efficiently. Robust cybersecurity solutions and consistent facility upgrades are the backbone of every safe-supporting banking process in today's technological landscape.

REFERENCES

[1] Charles P. Pfleeger, and Shari Lawrence, *Security in Computing*, 5th ed., Prentice Hall, USA, 2015.
[2] Nina Godbole, and Sunit Belapure, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India Pvt Ltd, New Delhi, 2011.
[3] Joseph Migga Kizza, *Guide to Computer Network Security*, Springer Publications, USA, 2020.
[4] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, New York, 2015.
[5] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2020.
[6] Michael E. Whitman, and Herbert J. Mattord, *Principles of Information Security*, 7th ed., Cengage Learning, USA, 2023.
[7] J. Andress, The basics of information security : understanding the fundamentals of InfoSec in theory and practice. Waltham, Ma: Syngress ; Amsterdam, 2014.
[8] J. Katz, Introduction To Modern Cryptography. CRC Press, 2019.
[9] G. Mcgraw, Software security : building security in. Upper Saddle River, NJ: Addison-Wesley, 2006.