International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 3 , March 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos03032658456

Cybersecurity Challenges in Modern Technology

Dharshini M[1], Devibala S[2]
[1,2] PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science.

Article Info

Article History:

Published:19 March 2026

Publication Issue:
Volume 3, Issue 3
March-2026

Page Number:
371-376

Corresponding Author:
Dharshini M

Abstract:

Cybersecurity has become one of the most important aspects of modern technology as digital systems, networks, and online services continue to grow rapidly. Organizations, businesses, and individuals increasingly rely on the internet for communication, data storage, financial transactions, and information sharing.
However, this rapid digital transformation has also increased the risk of cyber threats such as hacking, malware attacks, phishing, ransomware, and data breaches. These cyber attacks can cause serious damage including financial loss, data theft, privacy violations, and disruption of services. Modern cybersecurity focuses on protecting computer systems, networks, and sensitive information from unauthorized access and malicious activities. Various security techniques such as encryption, firewalls, intrusion detection systems, and multi-factor authentication are used to strengthen digital protection. Despite these measures, cybercriminals continuously develop new and advanced attack methods, making cybersecurity a constant challenge for organizations. This study discusses the major cybersecurity challenges in modern technology, existing security approaches, ethical concerns, and future developments in the field of cybersecurity.

Keywords: Cybersecurity

1. Introduction

Cybersecurity refers to the practice of protecting computer systems, networks, and digital data from cyber threats and unauthorized access. With the rapid development of modern technologies such as cloud computing, mobile devices, and online services, large amounts of sensitive information are being stored and transmitted over the internet. This has increased the importance of cybersecurity in protecting personal, organizational, and government data.

Cyber attacks such as phishing, ransomware, and hacking have become more common and sophisticated, creating serious risks for individuals and businesses. Effective cybersecurity strategies help prevent data breaches, protect privacy, and ensure the safe operation of digital systems.

As technology continues to evolve, organizations must continuously improve their security systems and adopt new technologies to defend against emerging cyber threats.

2. Literature Review

Many researchers have studied cybersecurity and its importance in protecting modern digital systems. Earlier studies mainly focused on basic network security techniques such as firewalls and antivirus software to prevent cyber attacks.

However, as technology advanced, cyber threats also became more complex and difficult to detect. Recent research highlights the increasing use of advanced security techniques such as artificial intelligence, machine learning, and behavioral analysis to detect and prevent cyber attacks.

Several studies also emphasize the importance of user awareness and proper security policies to reduce human-related security risks. Researchers agree that a combination of technical solutions, security policies, and user education is necessary to create an effective cybersecurity system.

Objectives of the Study

The main objectives of this study are:

To understand the concept of cybersecurity and its importance in protecting modern digital systems and networks.

To identify the major cybersecurity challenges faced by organizations and individuals in the digital environment.

To analyze different cybersecurity techniques and tools used to protect data, networks, and computer systems from cyber attacks.

To examine security risks and ethical issues related to data privacy, information protection, and responsible use of technology.

To explore future developments and trends in cybersecurity that can improve protection against advanced cyber threats.

3. Research Methodology

The research methodology for this study focuses on understanding the role of cybersecurity in financial management and identifying the major cyber threats faced by financial systems.

The study is based on collecting information from academic journals, research papers, books, and reliable online sources related to cybersecurity and financial management.

These sources help in analyzing the importance of security measures in protecting financial data and digital transactions.

The research follows a descriptive approach to examine different cybersecurity techniques used in financial institutions.

Methods such as data encryption, authentication systems, firewalls, and fraud detection technologies are studied to understand how they protect financial systems from cyber attacks. The study also reviews existing financial security practices used by banks and financial organizations.

Cyber Security in Financial Management

A. Protection of financial Data

Cybersecurity helps protect sensitive financial information such as bank details, transaction records, and customer data from unauthorized access and cyber attacks

B. Prevention of Fraud and Cyber Attacks

Financial institutions use cybersecurity systems to prevent fraud, phishing, hacking, and ransomware attacks that may lead to financial losses.

C. Secure Online Transactions

Cybersecurity ensures safe online banking, digital payments, and financial transactions by using encryption and authentication technologies.

D. Data Privacy and Confidentiality

It helps maintain the privacy and confidentiality of financial data, ensuring that only authorized users can access important financial information.

Cyber security in Financial Decision-Making

Protection of Financial Information

Cybersecurity helps protect sensitive financial data such as investment records, financial reports, and strategic plans from cyber attacks and unauthorized access.

Secure Data for Decision Making

Financial decisions depend on accurate and reliable data. Cybersecurity ensures that financial information is protected from manipulation, loss, or corruption.

Prevention of Financial Fraud

Cybersecurity systems help detect and prevent fraudulent activities such as hacking, phishing, and identity theft that could influence financial decisions.

Risk Management

Cybersecurity helps financial managers identify cyber risks that may affect financial planning, investments, and business strategies.

Confidentiality of Financial Strategies

Organizations often keep financial plans and investment strategies confidential. Cybersecurity protects these important decisions from being leaked or stolen.

Cyber Security Applications Across Financial Functions

A. Accounting and Financial Reporting

Cybersecurity protects accounting systems and financial reports from unauthorized access, data manipulation, and cyber attacks, ensuring accurate financial information.

B. Budgeting and Financial Planning

Secure systems help protect budgeting data and financial planning information from cyber threats, allowing organizations to make reliable financial plans.

C. Banking and Payment Systems

Cybersecurity ensures safe online banking, digital payments, and fund transfers by protecting financial transactions from hacking, fraud, and phishing attacks.

Impact on Organizational Performance

Improved Operational Efficiency

Cybersecurity helps organizations maintain smooth operations by protecting systems from cyber attacks that may disrupt business activities.

Protection of Organizational Data

Strong cybersecurity measures protect important organizational data such as financial records, customer information, and strategic plans from unauthorized access.

Increased Customer Trust

When organizations protect customer data effectively, it builds trust and confidence among customers and improves the organization's reputation.

Reduced Financial Losses

Cyber attacks can cause financial losses due to fraud, data theft, or system downtime. Effective cybersecurity helps reduce these risks and protect organizational assets.

Challenges and Ethical Considerations

Cyber Attacks and Fraud

Financial systems are often targeted by cybercriminals through phishing, hacking, malware, and ransomware attacks.

Data Breaches

Unauthorized access to financial databases can lead to theft of sensitive financial and customer information.

System Vulnerabilities

Weak security systems or outdated software can create vulnerabilities that cyber attackers may exploit.

Human Error

Employees or users may unintentionally expose financial data through weak passwords, unsafe internet usage, or lack of cybersecurity awareness.

Rapidly Evolving Threats

Cyber threats are continuously evolving, making it difficult for organizations to keep their security systems fully updated.

4. Future Trends

Artificial Intelligence in Cybersecurity

Artificial Intelligence (AI) and machine learning will be widely used to detect cyber threats, analyze unusual activities, and prevent fraud in financial systems.

Blockchain Technology

Blockchain will improve security and transparency in financial transactions by providing a secure and decentralized system for storing financial records.

Biometric Authentication

Future financial systems will increasingly use biometric security methods such as fingerprint scanning, facial recognition, and voice recognition to improve authentication and access control.

5. Conclusion

Cybersecurity plays a vital role in protecting financial systems and ensuring secure financial management. With the increasing use of digital technologies in financial activities such as online banking, digital payments, and financial decision-making, the risk of cyber threats has also increased. Effective cybersecurity measures help protect sensitive financial data, prevent fraud, and maintain the stability of financial systems.

Financial organizations must implement strong security strategies such as encryption, authentication, and continuous monitoring to safeguard financial information.

In addition, ethical practices and compliance with legal regulations are important to ensure responsible handling of financial data and to maintain customer trust.

In conclusion, cybersecurity is essential for the safe operation of financial systems. As technology continues to evolve, organizations must adopt advanced security technologies and improve cybersecurity awareness to protect financial information and support secure financial management in the future.

References

1. William Stallings (2018). Network Security Essentials: Applications and Standards. Pearson.
2. Joseph Migga Kizza (2020). Guide to Computer Network Security. Springer.
3. Nina Godbole & Sunit Belapure (2011). Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Wiley India.
4. International Organization for Standardization (ISO). Information Security Management Standards (ISO/IEC 27001).