

Original Article**Cyber security: Challenges, Threats and Modern Solutions****Mulla Tausif Sileman**

Adarsh College, Vita, Department:- Computer Science

Email: mullatausif891@gmail.com**Manuscript ID:**
CSJ-2026-020506

Volume 2

Issue 5

Pp. 22-26

October 2026

ISSN: 3067-3089

Submitted: 08 Sept. 2026**Revised:** 16 Sept. 2026**Accepted:** 05 Oct. 2026**Published:** 31 Oct. 2026**Correspondence Address:**Mulla Tausif Sileman
Adarsh College, Vita, Department:-
Computer Science
Email: mullatausif891@gmail.com

Quick Response Code:

Web: <https://csjour.com/>

DOI: 10.5281/zenodo.22952763

DOI Link:

<https://doi.org/10.5281/zenodo.22952763>

Creative Commons

**Abstract**

Cyber security is the practice of protecting computers, networks, software, systems, and data from unauthorized access, attacks, damage, or disruption. With the rapid growth of the Internet, cloud computing, mobile devices, and artificial intelligence, more chances cyber threats are becoming more complex. Common threats include phishing, malware, ransomware, password attacks, denial-of-service attacks, man in middle attacks, and data breaches. This research paper discusses major cybersecurity threats, their impact, existing security techniques, and the role of Artificial Intelligence and Machine Learning in improving cyber defense. The paper also discusses challenges and effects and future directions for building safer digital systems.

Keywords: Cybersecurity, Machine Learning, Artificial Intelligence, Malware, Phishing, Ransomware, Network Security, Data Protection

Introduction

The increasing use of digital technology has made cybersecurity an important requirement for individuals, businesses, educational institutions, governments, and other organizations. Large amounts of personal and organizational information are stored and transferred through digital networks.

Cyberattacks can result in financial losses, privacy violations, service interruptions, and damage to an organization's reputation. Therefore, effective cybersecurity requires a combination of technology, security policies, user awareness, and continuous monitoring.

Objectives

The main objectives of this research are:

- To understand the concept and importance of cybersecurity.
- To identify common types of cyber threats.
- To study the impact of cyberattacks.
- To examine modern cybersecurity technologies.
- To study the application of AI and ML in cybersecurity.
- To identify major challenges in implementing cybersecurity.

Objectives

The main objectives of this research are:

- To understand the concept and importance of cybersecurity.
- To identify common types of cyber threats.
- To study the impact of cyberattacks.
- To examine modern cybersecurity technologies.
- To study the application of AI and ML in cybersecurity.
- To identify major challenges in implementing cybersecurity.
- To suggest possible future improvements.

Major Cybersecurity Threats**Phishing**

Phishing is a technique in which attackers use fraudulent emails, messages, or websites to trick users into revealing sensitive information such as passwords or financial details.

Malware

Malware is malicious software designed to damage systems, steal information, or obtain unauthorized access. Examples include viruses, worms, trojans, and spyware.

Ransomware

Ransomware is a type of malware that prevents users from accessing their data or systems and demands payment from the victim.

Creative Commons (CC BY-NC-SA 4.0)

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-Non Commercial-ShareAlike 4.0 International Public License, which allows others to remix, tweak, and build upon the work no commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

How to cite this article:

Mulla, T. S. (2026). Cyber security: Challenges, Threats and Modern Solutions. Computer Science Journal, 2(5), 22–26. <https://doi.org/10.5281/zenodo.22952763>

Password Attacks

Attackers may attempt to obtain passwords through guessing, credential theft, brute-force attacks, or previously leaked credentials.

Denial-of-Service Attacks

A denial-of-service attack attempts to make a computer system or online service unavailable by overwhelming it with traffic or requests.

Man in middle Attacks

A man-in-the-middle attack also known as an on-path attack is a cyber threat where an unauthorized person secretly intercepts, reads, or alters communications between two parties who believe they are talking directly to each other

Data Breaches

A data breach occurs when unauthorized individuals gain access to confidential or sensitive information.

Role of Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning can help cybersecurity systems identify unusual patterns and detect potential attacks. ML models can be trained using network traffic, system logs, email characteristics,

URLs, and other security-related data. Possible applications include:

- Intrusion detection
- Malware classification
- Phishing detection
- Spam detection
- Fraud detection
- Anomaly detection
- User behavior analysis

Machine learning can improve automated detection, but ML systems themselves must be protected against manipulation and poor-quality training data.

Cybersecurity Methodology

A typical AI-based cybersecurity research project can follow these steps:

Data Collection → Data Preprocessing → Feature Selection → Model Training → Testing → Performance Evaluation → Threat Detection

For an intrusion-detection study, publicly available cybersecurity datasets can be used. Algorithms such as Random Forest, Support Vector Machine, Decision Tree, XGBoost, or neural networks can then be compared.

Evaluation Parameters

The performance of a cybersecurity ML model can be evaluated using:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate
- False Negative Rate
- Detection Rate

Accuracy alone should not be used to judge a security model, especially when normal and attack samples are highly imbalanced.

Challenges:Core Challenges

- **Expanded Attack Surfaces:** The rapid growth of cloud computing, multi-cloud setups, and Internet of Things (IoT) devices blurs traditional network perimeters.
- **Skills Shortage:** Organizations globally struggle with a severe deficit of trained cybersecurity professionals.
- **Human Error:** Inadvertent user mistakes and poor security hygiene remain primary entry points for threat actors.
- **AI-Driven Attacks:** Malicious operators increasingly use artificial intelligence to automate and accelerate offensive maneuvers.
- **Modern Solutions**
- **Zero Trust Architecture:** Organizations adopt strict verification models that require continuous validation for every user and device trying to access resources.
- **AI and Machine Learning Defense:** Security teams deploy automated threat detection systems to analyze massive network flows and spot anomalies in real time.
- **Identity and Access Management (IAM):** Advanced multi-factor authentication (MFA) and granular authorization boundaries limit lateral movement.
- **Security Information and Event Management (SIEM):** Centralized logging and threat intelligence platforms improve visibility across complex hybrid environments

Some important cybersecurity challenges include:

- Rapidly changing attack techniques.
- Increasing volume of security data.
- Shortage of cybersecurity professionals.
- Privacy and data-protection requirements.
- False alarms from security systems.
- Difficulty detecting previously unknown attacks.

- Security risks associated with AI systems themselves.

Future Scope

- Future cybersecurity research can focus on:
- AI-powered real-time threat detection.
- Explainable AI for security decisions.
- Privacy-preserving machine learning.
- Federated learning for cybersecurity.
- Automated incident response.
- Detection of AI-generated phishing and social engineering.
- Robust ML models resistant to adversarial attacks.
- Security for Internet of Things devices.

Solutions

Advanced Cybersecurity Solutions



- This diagram shows **8 major cybersecurity technologies** working together to protect an organization's **devices, network, applications, users, and data**.
- **layered security system:** different tools protect different parts of the environment, and some of them share information so the security team can detect and respond to attacks immediately.

DLP — Data Loss Prevention

The diagram ask:

“Protects sensitive data”

DLP can identify sensitive information and help prevent unauthorized transfer or

. EDR/XDR -EDR = Endpoint Detection and Response

- **XDR = Extended Detection and Response**

The diagram dscribe:

“Detects and responds to threats”

EDR focuses primarily on **endpoints** such as:

Laptops,Desktop computers,Servers,Workstations,Other managed devices

It continuously monitors endpoint activity and can detect suspicious behavior, investigate it, and isolate affected systems.

EDR = security camera inside a computer.

XDR = security control room watching the entire organization.

IPS - Intrusion Prevention System

- **IPS = Intrusion Prevention System**

The diagram says:

“Monitors network traffic”

An IPS examines network traffic looking for malicious activity and can **actively block** detected threats.

NGFW - Next-Generation Firewall

NGFW = Next-Generation Firewall

The diagram says:

“Advanced filtering capabilities”

A traditional firewall primarily controls traffic based on things such as:

Source IP, Destination IP, Port, Protocol, An NGFW provides more advanced security capabilities and is designed to address modern threats.

Depending on the product, it can incorporate capabilities such as:

Application control, User-based policies, URL/web filtering, Intrusion prevention, Malware protection

SSL/TLS inspection

Threat intelligence

Advanced traffic filtering

A traditional firewall is like a **security guard checking IDs**.

An NGFW is like a **security guard + baggage scanner + behavioral monitoring system**.

SASE -Secure Access Service Edge

The diagram says:

“Integrates network and security”

SASE is different from the other technologies because it is primarily an **architecture/service model** rather than just one security appliance.

SASE combines networking capabilities with cloud-delivered security services. It is designed particularly for environments where users and applications can be anywhere.

SASE can evaluate things such as:

User identity, Device, Location, Application, Security posture, Access policy, Network conditions, Technologies commonly associated with SASE

SASE can incorporate:

SD-WAN

Secure Web Gateway (SWG)

Zero Trust Network Access (ZTNA)

Cloud Access Security Broker (CASB)

Firewall-as-a-Service

DLP

SIEM — Security Information and Event Management

SIEM = Security Information and Event Management

The diagram says:

“Analyzes security data”

SIEM is essentially a **central security monitoring and analysis platform**.

It collects logs and security events from many different systems:

But the SIEM can correlate them and conclude:

SOAR - Security Orchestration, Automation and Response

SOAR = Security Orchestration, Automation and Response

The diagram says:

“Automates security operations”

SOAR helps security teams **automate repetitive incident-response tasks**.

8. How all 8 technologies work together

This is the most important part of the diagram.

A useful way to remember the diagram is:

Conclusion

Cybersecurity has become essential because modern society increasingly depends on digital systems and online services. Traditional security techniques remain important, but attackers continue to develop new methods. Artificial Intelligence and Machine Learning provide promising approaches for detecting suspicious behavior and automating parts of cyber defense. However, AI should be combined with strong security practices, human expertise, privacy protection, and continuous monitoring. Future research should focus on developing accurate, explainable, robust, and privacy-preserving cybersecurity systems.

Acknowledgement

I would like to express my sincere gratitude to everyone who supported and guided me in completing this research paper entitled “Cyber Security: Challenges, Threats and Modern Solutions.” The study focuses on major cybersecurity threats, the role of Artificial Intelligence and Machine Learning, modern security technologies, and future approaches to strengthening digital security.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. NIST, Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology.
2. NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0).
3. ENISA, Threat Landscape, European Union Agency for Cybersecurity.
4. MITRE, ATT&CK Knowledge Base, MITRE Corporation.
5. ISO/IEC 27001, Information Security Management Systems — Requirements.