IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 4, Ser. 3 (July. – August. 2026), PP 36-40
www.iosrjournals.org

Cybersecurity in the Modern Digital Era: A Comprehensive Review of Emerging Threats, Defense Mechanisms, and Future Perspectives

Somnath Kar[1], Saurav Sinha[2], Anand Kumar Sinha[2], Radheshyam Mahato[2]
[1.] *University Department of Physics, Kolhan University Chaibasa, Jharkhand, India*
[2.] *University Department of Computer Applications((MCA), Kolhan University, Chaibasa, Jharkhand, India*

Abstract
Digital technologies have improved significantly over the last few decades. While technologies like Artificial Intelligence (AI), Machine Learning, Internet of Things (IoT) have improved individuals and society as a whole, it has also invited new and advanced methods of cyberattacks. Cyberattacks are no more about attacking individual systems or networks, it has become very organized using technologies like AI, deepfake, etc. to attack government, businesses, financial institutions and critical infrastructures like atomic and nuclear plants.The study is based on qualitative review methodology where we do systematic analysis of peer-reviewed literature, government records, and other international standard publications.As a result, the findings suggest that traditional security models are not sufficient to tackle the advanced cyber threats. Hence, we need a combination of emerging technologies like Artificial Intelligence, ML, Blockchain technology, Security Information & Event Management (SIEM), Zero Trust Architecture to deal with problems of modern cybersecurity challenges.
Additionally, a concept of Integrated Adaptive Cybersecurity Framework (IACF) is proposed to develop an integrated cybersecurity strategy.

Keywords
Cybersecurity; Artificial Intelligence; Zero Trust Architecture; Cloud Security; Internet of Things; Cyber Threats; Information Security

---

Date of Submission: 15-08-2026 Date of Acceptance: 31-08-2026

I. INTRODUCTION

Ever since the introduction of internet, computers or other devices connected to it have always been at a risk of being misused at the hands of some third person, who may use the network to access systems without authority. However, since now every sector ranging from a simple grocery store to a big corporate office and from a local government office to a large organisation like Atomic & Nuclear head with sensitive data have completely been dependent on internet for their day-to-day functioning, therefore it becomes very important to protect these from modern emerging cyberattacks which are way advanced & organized compared to what cyberattacks used to be a decade before. Modern cyberattacks use technologies like Artificial Intelligence, deepfake, identity theft etc. to gain access to just any system.

Recent Ransomware attack in AIIMS Delhi in 2022 showed how difficult it became to manage patients & hospital offline.

However, the good thing is, using the same technologies like Artificial Intelligence, Machine Learning along with Blockchain, Zero Trust Architecture, Multi-factor authentication etc. we can tackle these modern cyberattacks.

This paper at the end suggests an integrated approach called "Integrated Adaptive Cybersecurity Framework (IACF)" that combines technologies which is a combined policy involving technologies to handle cyberattacks, human-response & government policy and framework.

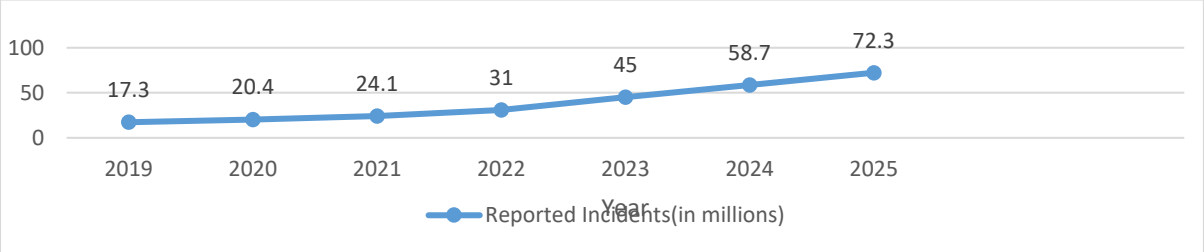

Figure 1: Worldwide cyberattack trend(2019-2025)
Source: Statista – CyberAttacks & data breaches worldwide from 2019 to 2025

II. LITERATURE REVIEW

Due to rapidly evolving technologies and modernised cybersecurity threats arising from it, cybersecurity has become an attractive topic for research. While studies a couple of years ago focused more on detecting malware, preventing phishing, security of IoT & cloud networks, the shift in the recent time has moved a lot towards understanding cyberthreats using emerging technologies like AI & ML and solving the problem..

Research Gap

Despite all the researches conducted, we still have very few research focused on developing a unified scheme that covers all the tech, the individual role & responsibility and government & corporate rules & regulation. This paper proposes an Integrated Adaptive Cybersecurity Framework (IACF) for the same.

Table 1 Comparative Summary of Selected Literature

Author(s)/Source	Primary Focus	Key Contribution	Research Limitation
NIST (2024)	Cybersecurity Framework	Risk-based cybersecurity governance	Limited implementation guidance for specific sectors
Verizon DBIR (2024)	Data breach analysis	Global trends in cyber incidents	Focuses primarily on reported breaches
IBM Security (2024)	Data breach studies	Analysis of financial impact of cyberattacks	Industry-focused observations
OWASP (2021)	Web application security	Identification of critical web vulnerabilities	Limited coverage beyond web applications
Recent AI-based Studies	Intelligent threat detection	Automation and behavioural analytics	Primarily technology-specific
Recent Zero Trust Studies	Identity-centric security	Continuous authentication and least-privilege access	Implementation complexity

III. RESEARCH METHODOLOGY

We have done a qualitative review of primary work done by various groups. The secondary data was collected from sources like NIST, ISO, IBM security, OWASP etc. The data taken for review is mostly of the duration between 2021–2024.

Research methodology → Literature search → source selection → quality screening → thematic classification → comparative analysis → key findings & research gap → proposed IACF

IV. CYBERSECURITY THREAT LANDSCAPE

Widespread expansion of AI, IoT and other digital services have significantly increased complexity of the nature of the cyberattacks.

Malware being one of the oldest, yet prevalent cyber threat methods that consists of viruses, worms,spywares, trojans etc. to gain unauthorised access to system.

Ransomware on the other hand encrypts organisational data and demands payment often in means like bitcoins.

Another common cyberattack method is **Phishing** where fake emails, websites, deepfake videos are used to target human behaviour & steal credentials & do financial frauds.

At times, cyberattacks also happen due to **Insider Threats** where someone from the organisation compromises the system or access with cybersecurity. At the hardware & software level, **cloud misconfiguration,** compromised software supply chains & insecure IoT devices make organisations more vulnerable to risks of cyberattacks.

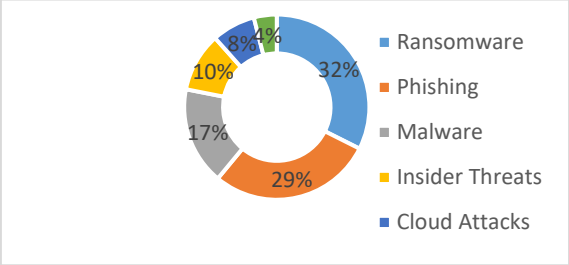

Figure 2 Distribution of Major Cyber Threats(2024)
Source: IBM Security-Cost of a Data Breach Report 2024

Table II. Comparative Analysis of Major Cybersecurity Threats

Threat Type	Primary Target	Major Impact	Recommended Mitigation
Malware	End-user devices	System compromise and data theft	Endpoint protection and software updates
Ransomware	Organizations	Data encryption and service disruption	Regular backups and EDR
Phishing	Users and enterprises	Credential theft and financial fraud	MFA and security awareness
Insider Threat	Organizational resources	Data leakage and misuse	Least-privilege access and monitoring
Cloud Attacks	Cloud infrastructure	Unauthorized access and data breaches	Cloud security monitoring
IoT Attacks	Connected devices	Network compromise and service disruption	Secure configuration and firmware updates
Supply Chain Attacks	Software ecosystems	Widespread organizational compromise	Vendor risk assessment and software verification

V. MODERN CYBERSECURITY DEFENSE MECHANISMS

Since traditional methods are not enough to counter emerging cyber threats, we nowadays use a combination of multilayer defence strategies that does behavioural analysis of threats to automatically detect and process it. The multilayered approach includes:-

A. Artificial Intelligence & Machine Learning that helps identify threats by analysing its behaviour & pattern across a large volume of data.

B. Zero Trust Architecture where we don't trust any device or user by default and use methods like role based access and multifactor authentication to allow access.

C. Another cyber defence mechanism includes **Blockchain technology** to improve data integrity by decentralising record management**. Security & Event Management (SIEM)** to continuously monitor the incident response to know security alerts.

Table III. Comparison of Modern Cybersecurity Defense Mechanisms

Technology	Primary Function	Key Advantage	Typical Application
AI & Machine Learning	Intelligent threat detection	Detects known and unknown attacks	Malware detection and anomaly analysis
Zero Trust Architecture	Continuous identity verification	Reduces unauthorized access	Enterprise and cloud security
Multi-Factor Authentication	User authentication	Strengthens account security	Identity and access management
Blockchain	Data integrity and trust	Tamper-resistant records	Secure transactions and audit trails
SIEM	Security monitoring	Centralized event analysis	Security Operations Centers (SOC)
Encryption	Data confidentiality	Protects sensitive information	Secure communication and cloud storage

VI. CASE STUDIES OF MAJOR CYBERSECURITY INCIDENTS

We have examples from our recent past that demonstrates how successful attacks exploit a combination of vulnerabilities at different levels and exposes not just human errors, but also organisational weaknesses.

The WannaCry Ransomware (2017) simultaneously attacked thousands of computers across various entities by exploiting vulnerabilities of unpatched Microsoft Windows system.

The SolarWinds supply chain attack (2020), on the other hand compromised trusted software updates, raising a question on the authenticity of vendors supplying the software.
A ransomware attack on Colonial Pipeline system known **by Colonial Pipeline attack (2021**) disrupted fuel supply across America, similarly in India in 2022, a ransomware attack on AIIMS Delhi, known by **AIIMS New Delhi cyberattack (2022)** showed how functioning of a hospital system can be disrupted by a cyberattack.

Table IV. Comparative Analysis of Major Cybersecurity Incidents

Incident	Year	Primary Attack	Impact	Key Lesson
WannaCry	2017	Ransomware	Global service disruption	Timely patch management and backups
SolarWinds	2020	Supply Chain	Compromised trusted software	Vendor risk management
Colonial Pipeline	2021	Ransomware	Critical infrastructure disruption	Business continuity planning
AIIMS New Delhi	2022	Data Breach/Ransomware	Healthcare service disruption	Strengthen cybersecurity in public institutions

VII. INDIA'S CYBERSECURITY FRAMEWORK

While initiatives like Digital India, e-governance, UPI and digital banking have enhanced the system, it has also increased the need for a strong cybersecurity mechanism. We have IT Act 2000, the DPDP Act 2023 on one hand to deal with governance and legal frameworks. On the other hand we have CERT-In that deal with response to organisational cyberattacks. CERT-In also issues regular advisory to promote awareness.

Component	Primary Role
IT Act, 2000	Legal framework for cyber offences and electronic governance
DPDP Act, 2023	Protection of personal digital data and privacy
CERT-In	National incident response and cybersecurity coordination
NCIIPC	Protection of critical information infrastructure
Digital India	Promotion of secure digital governance and public services
National Cyber Security Policy	Strategic guidance for national cybersecurity

VIII. EMERGING TRENDS AND FUTURE RESEARCH DIRECTIONS

Future trends in cybersecurity focus on more intelligent automation, adaptive to environment and more proactive risk management procedures.
Most important trends would include:

- **AI-driven cybersecurity**, where AI trained models will become more advanced to identify and clarify cyberthreats.
- We will have **quantum safe security** to deal with cyberthreat challenges to current cryptographic algorithms.

We will also have more methods to deal with **cloud & IoT security** as well as human-centric cybersecurity challenges.

Table V. Emerging Trends and Future Research Directions

Emerging Trend	Future Focus	Expected Impact
Artificial Intelligence	Detection of predictable threat	Quick and concise response
Quantum Computing	Cryptography after quantum	encrypted data be protected at long time
Cl		
Cybersecurity Governance	International standards and regulations	organisational resilience becomes better
Human-Centric Security	Spread awareness, training and cyber ethics	fewer social engineering attacks

IX. PROPOSED INTEGRATED ADAPTIVE CYBERSECURITY FRAMEWORK (IACF)

As a result of the findings, we observe that it is not possible to counter modern day cyberthreats either by technologies or law alone. So what we need is an integrated scheme that includes all. The tech to detect & fight cyberattacks, the law & governance, user awareness etc. The integrated scheme proposed is called "Integrated Adaptive Cybersecurity Framework (IACF)" that has five framework layers:-
(i) Intelligent threat detection (ii) Identity and access security (iii) Infrastructure protection (iv) Governance & compliance (v) Human-centric security

Table VI. Components of the Proposed IACF

Framework Layer	**Primary Objective**	**Key Technologies/Practices**
Threat Detection intelligently	cyber threats identification proactively	Artificial intelligence, ML, SIEM
Access Security And Identity	Prevention of unauthorized access	Zero Trust, RBAC
Infrastructure Protection	Secure digital assets	Cloud Security, IoT Security, Encryption
Governance & Compliance	Regulatory manages operations	NIST, CERT-In, ISO, IEC
Human-Centred Security	Reduce human-related cyber risks	Awareness, Training, Security Culture

X. CONCLUSION

The need for cybersecurity in modern digital ecosystem is the necessity we can't ignore, specially when we have time to time seen how organised cyberattacks have affected the working of hospitals, banks & other organisations affecting economy at large. As the nature of cyberattacks become advanced, we also need to improve our defence mechanisms. Throughout our findings, we find that neither traditional methods nor the AI & ML models in standalone basis are enough to handle these cyber threats. Consequently, we suggest using an integrated approach we have named “Integrated Adaptive Security Framework”(IACF) where technologies, governance, policies and human practices are all combined to deal with emerging cyberthreats.

REFERENCES

[1]. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," Version 2.0, Gaithersburg, MD, USA, 2024.
[2]. Verizon, "2024 Data Breach Investigations Report (DBIR)," Verizon Enterprise, 2024.
[3]. IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, 2024.
[4]. OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.
[5]. Computer Emergency Response Team-India (CERT-In), "Annual Report," Ministry of Electronics and Information Technology, Government of India, 2023.
[6]. Government of India, "Information Technology Act, 2000," New Delhi, India.
[7]. Government of India, "Digital Personal Data Protection Act, 2023," Ministry of Electronics and Information Technology, New Delhi, India.
[8]. Cisco Systems, "Cisco Cybersecurity Readiness Index 2024," Cisco, 2024.
[9]. W. Stallings, Network Security Essentials: Applications and Standards, 7th ed., Pearson, 2023.
[10]. D. Easttom, Modern Cryptography: Applied Mathematics for Encryption and Information Security, Springer, 2021.
[11]. M. Bishop, Computer Security: Art and Science, 2nd ed., Addison-Wesley, 2019.
[12]. IEEE Computer Society, "IEEE Transactions on Dependable and Secure Computing," Various Issues, 2022–2024.
[13]. ACM Computing Surveys, "Recent Advances in Cybersecurity Research," Various Issues, 2022–2024.
[14]. Google Cloud, "Cloud Security Best Practices," Google Cloud Documentation, 2024.
[15]. Amazon Web Services (AWS), "AWS Security Best Practices," AWS Whitepaper, 2024.
[16]. CrowdStrike, "Global Threat Report 2024," CrowdStrike, 2024.