Archives available at journals.mriindia.com

International Journal of Advanced Scientific Research and Engineering Trends

ISSN: 2456-0774

Volume 10 Issue 05, 2026

Artificial Intelligence for Enhancing Cybersecurity

[1]Mayuri M. Patil, [2]Vaishanvi J. Davari, [3]Jyoti B. Shinde
[1,2,3] Assistant Professor. Department of Computer Science, SVLM Titave

Peer Review Information

Submission: 15 April 2026

Revision: 27 April 2026

Acceptance: 09 May 2026

Keywords

Artificial Intelligence, Cybersecurity, Machine Learning, Deep Learning, Behavioral Analytics

Abstract

The rapid growth of digital systems and networked infrastructures has significantly increased the complexity and frequency of cyber threats. Cybersecurity is a fast-growing field of IT with reducing organizations' risk of hacks or data. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as health care, finance, and retail. The internet has revolutionized the way we communicate and conduct business. However, this revolution has come with a cost the emergence of cyber threats that can compromise our security and privacy. In this paper examines the application of AI techniques, including machine learning, deep learning, and behavioral analytics, in cyber security systems. It explores how AI can be used for current state of cyber security, discussing the threats posed by malicious actors, the technologies used to protect against them, and best practices for individuals and organizations to ensure their security. Furthermore, this paper explores the need for organizations and governments to work together to increase cyber security in the digital age. The paper also discusses the challenges associated with AI-driven cybersecurity, such as data quality, model interpretability, adversarial attacks, and ethical concerns.

Introduction

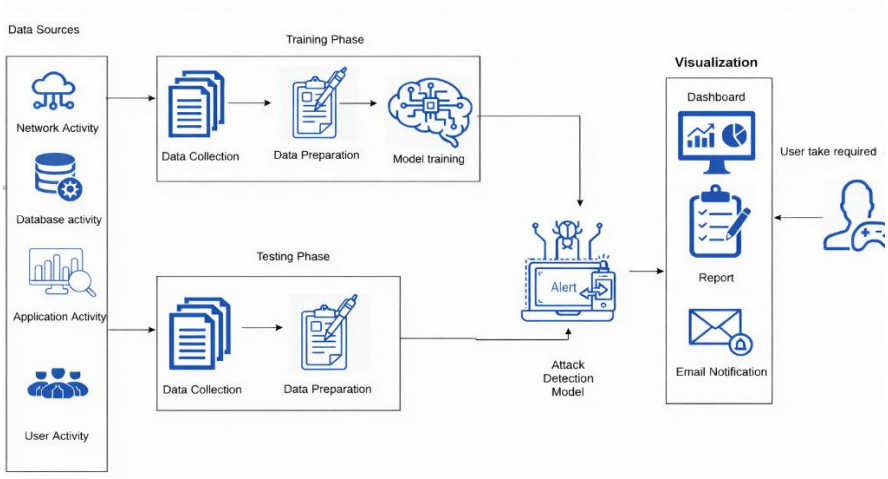
In today's digital age, cybersecurity has become a critical concern for individuals, businesses, and governments alike.

The rapid development of technology and the internet has brought many benefits to our lives, but it has also created new challenges, particularly in the realm of cyber security. Cybersecurity is defined as the practice of protecting networks, digital systems, and devices from theft, unauthorized access, and damage. This paper will explore the different aspects of cybersecurity, including the challenges it poses, the various cyber threats, and the measures taken to mitigate these threats. recent advancements and future research directions are highlighted to demonstrate how AI can play a critical role in scalable, building robust, and proactive cybersecurity solutions. The findings indicate that AI-based security systems significantly improve detection accuracy and response time, making them essential for protecting modern digital environments. Artificial Intelligence (AI) has emerged as a powerful solution to enhance cybersecurity by enabling adaptive, automated, and intelligent threat detection and response mechanisms.

The increasing support on digital technologies, cloud computing, and connected systems has transformed the path organizations process, and exchange information store. While this digital has improved efficiency and accessibility, it has also increse the attack surface for cyber threats. Cyberattacks such as ransomware, phishing, data breaches, malware infections, and advanced persistent threats (APTs) are becoming more frequent, costly , and complex, posing serious risks to organizations, individuals, and national security. As a result,

cybersecurity has become a critical concern in modern information systems.

Artificial Intelligence (AI) has emerged as a ensure approach to address the limitations of traditional cybersecurity techniques. By leveraging machine learning, deep learning, and data-driven models, AI-enabled security systems can analyze large-scale data, identify hidden patterns, and detect anomalous behavior in real time. These capabilities allow AI-based solutions to reduce false positives, detect cyber threats, and respond to incidents more efficiently than conventional methods. AI techniques are increasingly being applied in areas such as intrusion detection systems, vulnerability assessment, malware classification, phishing detection, and automated incident response. This paper aims to provide a comprehensive analysis of the role of Artificial Intelligence in enhancing cybersecurity. It examines key AI techniques and their applications in threat detection and prevention, discusses current challenges, and highlights future research directions. By exploring the medium between AI and cybersecurity, this study contributes to the development of intelligent, adaptive, and resilient security solutions capable of defending modern digital infrastructure.



Literature Review

Artificial Intelligence (AI), especially Machine Learning (ML) and advanced algorithms, has become a important component in modern cybersecurity research due to the increasing complexity and volume of cyber threats that traditional defense mechanisms are no longer fully capable of addressing. AI enables automation, pattern recognition, anomaly detection, and predictive defense strategies that are essential for protecting digital systems in real-time

1. Artificial Intelligence: A Modern Approach — Stuart J. Russell & Peter Norvig
2. Hacking: The Art of Exploitation — Jon Erickson
3. Cybersecurity for Dummies — Joseph Steinberg
4. The AI Journey — Suad Seferi

Existing Challenges

1. Data Quality and Availability –
   - Incomplete, noisy, and imbalanced datasets
   - Rapidly changing attack patterns that make datasets difficult.
   - Lack of labeled attack data due to privacy and confidentiality issue.
2. Evolving and Sophisticated Cyber Threats –
   - The dynamic nature of cyber threats makes it difficult for static AI models to remain effective over time.
   - Advanced Persistent Threats (APTs).
   - Polymorphic and metamorphic malware.
3. Adversarial Attacks on AI Models –
   - Craft adversarial inputs that evade detection.
   - Exploit model weaknesses to generate false negatives.
   - Such attacks compromise the reliability and trustworthiness of AI-based security solution.
4. Lack of Explainability and Transparency –
   - Makes it difficult for security analysts to understand decisions
   - Reduces trust in automated systems
   - Limits adoption in regulated industries
5. Privacy and Ethical Concerns –
   - Data privacy and user consent
   - Ethical use of surveillance technologies
   - Compliance with regulations such as GDPR

6. Shortage of Skilled Professionals –
   - Machine learning and data science
   - Network security and threat analysis
7. Integration with Existing Security Infrastructure –
   - Compatibility issues
   - High deployment and maintenance costs
   - Lack of standardization

Objectives of the Paper

1. To improve real-time threat detection and response.
2. To analyze existing cybersecurity threats and challenges.
3. To investigate the application of AI techniques in cybersecurity.
4. To identify limitations of current AI-based cybersecurity solutions.
5. To evaluate the performance of the proposed approach.
6. To propose an intelligent AI-based cybersecurity framework.
7. To enhance system adaptability against evolving attacks.
8. To address security, privacy, and ethical concerns.

1. Software and hardware used

- AI and Machine Learning Libraries
  - **NumPy** – Numerical computations and matrix operations
  - **Pandas** – Data preprocessing and feature engineering
  - **Scikit-learn** – Implementation of machine learning algorithms
  - **TensorFlow / PyTorch** – Development of deep learning models
  - **Matplotlib / Seaborn –** Visualization of results

- Cybersecurity Tools –
  - **Wireshark** – Network traffic capture and packet analysis
  - **Snort** – Intrusion detection and traffic monitoring
  - **SIEM tools** – Log collection and security event analysis
  - **Metasploit** – Simulation of cyber attacks for testing.

- Development and Experimentation Tools
  - **Anaconda** – Environment and package management
  - **Git/GitHub** – Version control and collaboration
  - **Jupyter Notebook** – Model development, testing, and visualization.

- Hardware Used

Processing Unit

- **CPU:** Intel Core i5/i7 or equivalent processor
- **GPU (Optional):** NVIDIA GPU for accelerating deep learning model training.

- Memory and Storage-
  - **RAM:** 8 GB or higher for efficient model
  - **Storage:** Minimum 256 GB HDD/SSD

Conclusion

India is at an important moment in using AI to predict and prevent cyber financial crimes. This paper has examined the role of Artificial Intelligence (AI) in enhancing cybersecurity by providing intelligent, adaptive, and automated defense solutions. AI learning model of NPCI and various state level projects show that India has both advanced technology and serious commitment to fighting online fraud.

The rapid growth of digital technologies and interconnected systems has significantly increased the frequency and sophistication of cyber threats, making traditional security mechanisms inadequate in many scenarios. Digital payment system in India is massive it handles nearly half of all real time transactions worldwide. Because the system is so large and processes payments so quickly it needs equally powerful mechanism to protect it. However advanced technology alone cannot guarantee fair and effective crime prevention. Using AI in policing and investigations must be supported by strong laws that ensure evidence is reliable complete constitutional protections for privacy and fair treatment and systems that ensure accountability and transparency. There are several problems right now like no clear rules for AI evidence in court, judges lacking the technical knowledge to evaluate AI systems, weak privacy protections when AI is used for surveillance and different regions having different abilities to analyze digital evidence.

These problems harm both how well AI systems work and constitutional rights of people. The Data Protection Act gives the government too many exemptions and has too few rules to hold AI systems accountable missing important chances to protect rights of people. The legal system of India is built on constitutional values like dignity, freedom and equality which provides a solid base for creating a unique way for India to regulate AI. One that uses new technology while protecting the basic rights of people. The suggested solutions including shared governance involving multiple groups, rules based on risk levels, forensic standards and legal changes provide a

plan for achieving this balance. As India continues to become more digital the decisions made today about using AI in law enforcement will affect not only how well crime is prevented but also the very nature of Indian democracy. The challenge is to make sure that AI is used as a tool for justice not just for speed and efficiency. AI should support human judgment while remaining accountable to human values and constitutional principles. Only by integrating AI in this balanced way can India unlock the full potential of AI while staying true to its commitment to justice, equality and human rights in the digital age.

References

Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver

Artificial intelligence for cybersecurity: a systematic mapping of literature

Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zh ang, K.K.R. Choo

Artificial intelligence in cyber security: research advances, challenges, and opportunities

T.C. Truong, I. Zelinka, J. Plucar, M. Čandík, V. Šulc

Artificial intelligence and cybersecurity: past, presence, and future

A.J. VarelaVaca, R.M. Gasca, R. Ceballos, M.T. Góm ez-López, P.B. Torres

CyberSPL: a framework for the verification of cybersecurity policy