Artificial Intelligence for Cybersecurity and protection of data

Prof. Hitesh Kaushal, Faculty Marketing Area, Aditya Institute of Management Studies and Research, (hiteshkaushal96@hotmail.com)

Dr. Aditya Desai, Faculty Information Systems and Operations Area, Aditya School of Business Management (aaditya.d@asbm.edu.in)

Abstract

AI in cybersecurity automates threat detection, improves response times, and strengthens defenses against emerging risks. Artificial Intelligence (AI) utilizes advanced algorithms and machine learning techniques to enhance the identification, prevention, and response to cyber threats.

As cyber threats continue to grow and surpass traditional security measures, hackers are constantly adapting their tactics, making the role of AI in cybersecurity more crucial than ever. AI helps prioritize critical incidents, detect threats in real-time, and automate responses to attacks, all while managing vulnerabilities and optimizing network security.

With AI-powered security automation, organizations can quickly identify anomalies, predict cyberattacks, and respond to threats more efficiently than human analysts. AI-based threat detection tools can analyze vast amounts of data, uncover zero-day vulnerabilities, and prevent AI-generated malware and phishing attacks from causing harm.

However, cybercriminals are also leveraging AI for malicious purposes, such as AI-driven brute-force attacks, deepfake phishing scams, and AI-powered DDoS attacks. This has led to an ongoing "AI arms race" between AI in cybersecurity and AI in cybercrime.

Keywords: Cybersecurity, Automation, Artificial Intelligence, Cybercrime

Introduction:

AI in cybersecurity automates threat detection, enhances response, and fortifies defences against evolving risks. Artificial Intelligence (AI) is about application of intelligent algorithms and machine learning techniques to enhance the detection, prevention, and response to cyber threats.

a. AI can be used to predict attack on the networks.
b. AI can detect anomaly in data which is harmful and need to be quarantined.

c. Additionally, Use of human experts to analyse the quarantined data.

Cyber threats are growing day by day and outpaces traditional security defences. Thousands of people are falling prey to cyberfraud’s and losing millions of rupees which is their hard-earned money. People across age groups spanning teenagers to senior citizens are part of the growing community of customers who have faced cyberfraud’s. Behind this evolution, Hackers are constantly shifting their focus, making AI in cybersecurity more important than it's ever been.

With the help of AI, we can prioritize critical incidents, detect threats in real-time, and respond to attacks automatically—all while managing vulnerabilities and optimizing network security.

Examples of cybercrimes - Data breach at ICICI Branch Indore where Lacs of rupees were transferred by bank employees using OTPs for transactions in customers' accounts in ICICI Bank's I-View software.

Literature Review

Artificial Intelligence in cybersecurity, Journal of Physics Conference series, Rammanohar Das and Raghav Sandhane

[1] Effectively securing cyberspace requires managing complex operations and vast amounts of information, a task unfeasible without significant automation. Traditional technologies and software, characterized by fixed, hardwired decision-making logic, face challenges in adapting to dynamic security threats. Artificial Intelligence (AI), particularly machine learning, offers solutions by introducing adaptability and simplicity.

This paper presents an overview of AI applications in cybersecurity, assessing how these technologies can enhance defense mechanisms. The review indicates that AI-driven tools, especially neural networks, are already protecting perimeters and addressing various cybersecurity challenges. However, certain issues, such as strategic decision-making requiring comprehensive information and logical decision support, remain unresolved and may benefit from AI approaches.

In summary, integrating AI into cybersecurity not only addresses current challenges but also holds promise for developing more resilient defense systems capable of adapting to evolving threats.

Cyber security meets artificial intelligence: a survey, School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China, Jian-hua LI

[2] The convergence of cybersecurity and artificial intelligence (AI) encompasses a broad spectrum of interdisciplinary interactions. On one side, AI technologies, such as deep learning, are integrated into cybersecurity to develop intelligent models for malware classification, intrusion detection, and threat intelligence sensing. Conversely, AI models themselves are susceptible to various cyber threats that can disrupt their sampling, learning processes, and decision-making abilities. Therefore, specialized cybersecurity defenses are essential to protect AI systems from adversarial attacks, preserve privacy in machine learning, and secure federated learning environments.

This paper provides a comprehensive review of the intersection between AI and cybersecurity. Initially, it summarizes existing research on combating cyber-attacks using AI, highlighting both traditional machine learning approaches and contemporary deep learning solutions. Subsequently, the paper analyses potential counterattacks against AI systems, examining their characteristics and classifying corresponding defense mechanisms. Finally, it explores research on constructing secure AI systems, focusing on the development of encrypted neural networks and the implementation of secure federated deep learning.

Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review, Debidutta Pattnaik a , Sougata Ray a , Raghu Raman

[3] This bibliometric review analyses the application of artificial intelligence (AI) and machine learning (ML) within the Banking, Financial Services, and Insurance (BFSI) sector. Focusing on Scopus-indexed articles, the study adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol, screening 39,498 articles and selecting 1,045 that met the inclusion criteria. N-gram analysis identified 177 unique terms in the titles and abstracts, while co-occurrence analysis uncovered nine distinct clusters, including fintech, risk management, anti-money laundering, and actuarial science. These clusters provide a comprehensive overview of the research landscape, highlighting areas for future exploration and informing study design. The findings offer valuable insights for policymakers, researchers, and practitioners in the BFSI sector, identifying research gaps and opportunities to enhance the sector's understanding and application of AI and ML technologies.

Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis,IEEE Access, HABIB ULLAH KHAN 1 , MUHAMMAD ZAIN MALIK1 , SHAH NAZIR2 , (Member, IEEE), AND FAHEEM KHAN

[4] Biometric authentication is gaining the interest of private, public, consumer electronics and corporate security systems. For the protection of cyberspace from hackers and other harmful people, biometric security is growing more and more popular among organizations, individuals and enterprises. The word "cyber security" refers to the procedures, techniques, and tools used to safeguard data, network system, computer networks and software from potential attacks online. Online financial service delivery is referred to as "cyber banking." As the trend of exchanging things has changed, internet banking has grown. Despite the benefits, there have been instances of security threat-related issues with Internet banking. To identify persons, biometric security verifies their physical attributes and behavioural traits. For identification verification, it is the most reliable and effective physical security method. According to biometric authentication, people can be recognized precisely based on their innate behavioural or physical traits. Numerous security measures have been implemented throughout the entire Internet banking service to address these issues. Globally, cybercrime has deep roots and poses a significant threat to the occurrence of criminal or terrorist behaviour. Without being addressed by a single authority, these risks can compromise security on the inside as well as the outside. If the cybercrime goes unnoticed, both money and personal data are lost. Internet services and information infrastructure have previously been targeted in assaults. Online fraud and hacker attacks are only two examples of the daily computer-related crimes that take place. The Internet of Things (IoT) is the most reliable foundation for facilitating high-quality, comfortable human living. IoT has had a substantial impact across a range of application domains. Smart gadgets are more vulnerable to hackers because of their rapid development and trust in wireless mechanics for data transport. As a result, the rate of cybercrime is rising daily. Artificial Intelligence (AI)-based cybersecurity emerges because of technological advancement and poses a risk to public safety, personal property rights, and privacy protection for people. The study elaborates on the key features of biometrics system in conventional and Islamic banking to counter the risk of cybersecurity and provide high safety and security to the banking industry. For this systematic literature review, the most

suitable and most relevant 101 articles from the reputed online libraries are selected. This analysis absorbed four research questions and pertinent keywords from the period of 2009 to 2022 (a part of 2023 was included).

Research Methodology: Data collection, tools, sampling methods.

- Data Collection: Mostly secondary Sources of Data and Journals
- Tools used: Variety of International Journals and proceedings of conferences were used for finding information related to the topic of research.

Results & Discussion:

The information presented clearly demonstrates the increasing reliance on Artificial Intelligence (AI) in cybersecurity, driven by the escalating sophistication of cyber threats.

- With AI-driven security automation, organizations can detect anomalies, predict cyberattacks, and respond to threats faster than human analysts.
- AI threat detection tools scan massive datasets, identify zero-day vulnerabilities, and neutralize AI-generated malware and phishing scams before they cause damage.
- Collection, Updating and Protection of customer data collected through marketing activities.
  a. IT act
  b. Issues related to data storage – collected from social media and other sources.
  c. What protocols to be followed for protection of data.
     i. First is protection of network – use of firewalls
     ii. Second is protection of data in encrypted form. if there is modification or changes in data store it can cause significant misinterpretation of data leading to false customer choices.
     iii. Third is prediction of attacks.
     iv. Intrusion detection systems
- **AI as a Critical Defense Tool:**
  - The text highlights that AI's ability to automate threat detection, predict attacks, and analyze vast datasets is

crucial for modern cybersecurity.

  - The literature review supports this, emphasizing AI's adaptability and its effectiveness in addressing complex security challenges.
  - The use of AI to analyze data and find anomalies, and then to quarantine the harmful data, before a human expert can check it, improves the speed of responses to attacks.

- **The "AI Arms Race":**
  - A significant finding is the recognition of the "AI arms race," where cybercriminals are also leveraging AI for malicious purposes. This underscores the need for continuous innovation in AI-powered defense mechanisms.
  - This shows that along with AI being used for good, it is also being used for bad, and thus, a constant state of improvement must be maintained.
- **Data Protection and Regulatory Compliance:**
  - The importance of data protection, adherence to regulations like the IT Act, and the implementation of robust security protocols (firewalls, encryption, intrusion detection) are emphasized.
  - The information about the ICICI bank data breach shows that data protection is still a major issue.
- **Financial Sector Applications:**
  - The literature review highlights the specific applications of AI and machine learning in the financial sector, including risk management, fraud detection, and biometric authentication.
  - Biometric security is shown to be a very useful tool in the banking sector.
- **Challenges and Future Directions:**
  - While AI offers significant advantages, challenges remain, such as protecting

    - AI systems from adversarial attacks and ensuring data privacy.
    - The research shows that AI is a tool that must be protected itself.

Conclusion:

The integration of AI into cybersecurity is essential for effectively combating evolving cyber threats. AI's capabilities in automation, threat prediction, and anomaly detection significantly enhance an organization's security posture. However, the dual use of AI by cybercriminals necessitates a continuous cycle of innovation and improvement.

Key conclusions include:

- AI plays a vital role in automating and enhancing cybersecurity defenses.
- The "AI arms race" requires ongoing development of advanced AI-powered security solutions.
- Robust data protection protocols and regulatory compliance are crucial.
- The financial sector benefits significantly from AI-driven security measures, especially biometric security.
- Future research should focus on addressing the challenges of protecting AI systems and ensuring data privacy.
- The use of AI allows for faster response times to cyber-attacks, and also allows for the prediction of future attacks.

In essence, AI is both a powerful weapon and a strong shield in the ongoing battle against cybercrime.

References:.

[1] Artificial Intelligence in cybersecurity, Journal of Physics Conference series, Rammanohar Das and Raghav Sandhane

[2] Cyber security meets artificial intelligence: a survey, School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China, Jian-hua LI

[3] Applications of artificial intelligence and machine learning in the financial services industry: A bibliometric review, Debidutta Pattnaik a , Sougata Ray a , Raghu Raman

[4] Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis, IEEE Access, Habib Ullah Khan 1 , Muhammad Zain Malik1 , Shah Nazir2 , (Member, IEEE), and Faheem Khan.

[5] MP News: Indore में ICICI बैंक मैनेजरों ने लगाई खातों में सेंध, खरीदा लाखों रुपए का सामान, Amar Ujala, Jan 8th, 2025