Journal of Advanced Zoology
ISSN: 0253-7214
Volume 44 Issue S-8 Year 2023 Page 69:72

Artificial Intelligence In Cyber Security

P. S. Dandge[1*], U. I. Dawre[2], R. F. Shirshikar[3]

[1*]*Department of Information Technology ,Changu Kana Thakur Arts, Commerce and Science College New Panvel, Maharashtra 410206, India. poojaghadage9145@gmail.com*
[2]*Department of Information Technology , Changu Kana Thakur ACS College New Panvel, Maharashtra 410206, India. umairdawre10@gmail.com*
[3]*Department of Information Technology, Changu Kana Thakur ACS College New Panvel, Autonomous Maharashtra 410206, India. raizan45@gmail.com*

***Corresponding Author:** P. S. Dandge*
poojaghadage9145@gmail.com

Abstract

As cyber threats continue to evolve in complexity and sophistication, the integration of artificial intelligence (AI) in cybersecurity has emerged as a critical frontier for enhancing threat detection, response, and mitigation strategies. This research paper provides a comprehensive examination of the current state of AI applications in cybersecurity, evaluating their strengths, weaknesses, and potential impact on the evolving threat landscape. The study employs a multidimensional methodology, incorporating a thorough literature review, case studies, interviews with cybersecurity experts, and analysis of real-world incidents

Keywords: Ai, Cyber Security

INTRODUCTION

Today, in cyber world where everything is digital & data is king. Data security (especially sensitive or personal data) is now more important than ever. Hackers are becoming smarter day by day & they are more innovative in exploiting the vulnerable data, organizations, and governments. With new cyberattacks, data bridges, & data breaches, data poisoning, hackers attacks, and crashes come to light almost every day. Cyber criminals pose a threat to organizations, businesses, governments who use computer networks. Cyber-attacks have been ranked as one of the top five most likely sources of global-scale risk. Attacks to networks are becoming more complex & cybercriminals are becoming more sophisticated every day. This compels organizations & others users of computer networks to pay close attention to their network security.

Cybersecurity refers to technology & practices designed to protect networks & information from damage or unauthorized access. It is vital because governments, companies, & military organizations collect, process, & store a lot of data. Cybersecurity takes different forms including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, & information systems. The cybersecurity is a dynamic field involving information systems, computer science, & criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, & integrity.

Cyber attacks are threatening the operation of businesses, banks, companies, & government networks. They vary from illegal crime of individual citizen to actions of groups, terrorists. Cyber attacks or threats include malware, phishing, denialof-service attacks, social engineering attacks, & man-in-the-middle attack. Cybersecurity involves reducing the risk of cyberattacks. Cyber risks should be manage proactively by

management. Cybersecurity technologies such as firewalls are widely available [2].

LITERATURE REVIEW

Ganesan. R. (2010): In his study he cautioned about spam mails sent by hackers. He introduces a new word scareware which is fake mail detecting software.
It cautions about all sort of communications over internet and warns not to open mails from open sources.
Govardhan. S. (2010): In his paper, he emphasized more on dynamic challenges faced by cyber security. In this day and age, hacker's intentions are malicious and to achieve it they are thinking out of box which a great threat for cyber security. He explained this by taking a classic example of operation aurora.
Selvakani, Maheshwari and Karavanasundari (2010): This study reveals the importance of cyber laws to protect the interest of cyber victims. AI should help in designing a strong law which can use effectively to trace cyber crimes.
Shukla R and Upadyaya A. (2011): This paper focuses more on financial data vulnerability. Now a day's people are more dependent on electronic banking activities. 90% of total commercial transactions are done online. Majority of cyber crimes are in banking industry only. Therefore this field requires high security and best practices.
Karheek D. N., Kumar M. A., Kumar M. R. P. (2012): This paper throws an attention in cryptographic measures. The basic problem in cryptography is security. By introducing new measures like quantum channel, cyber attacks can be reduced.
Balamuralikrishna I. T., Raghavendrasai, Sukumar S. (2012): It focuses on online frauds by various sites. In order to reduce the frauds the two techniques i.e. image matching and web page matching mechanism are helpful.

OBJECTIVES THE STUDY

- To examine the effectiveness of AI technologies in detecting and preventing cyber threats.
- To investigate how these technologies contribute to threat detection, incident response, and vulnerability analysis.
- To identify potential challenges and risks associated with the integration of AI in cybersecurity frameworks.
- To explore how AI can contribute to the proactive identification of emerging cyber threats.
- To evaluate the effectiveness of human-machine partnerships in incident response and decision-making.
- To explore privacy implications and potential biases in AI algorithms used for cybersecurity.

METHODOLOGY

Understanding the role of artificial intelligence (AI) in cybersecurity and the technologies employed to identify and prevent cyber attacks involves the collection and analysis of data related to cybersecurity incidents. This process often utilizes secondary data sources, such as incident reports, threat intelligence feeds, and publicly available information. In conjunction with the collection of this data, statistical tools, including measures of central tendency (simple and weighted averages) and percentile analysis, are applied to extract valuable insights.

- **Algorithmic Analysis:**

Definition: Analyzing the algorithms used in AI models to understand their efficiency, complexity, and computational requirements.
Application: Algorithmic analysis is crucial for assessing the scalability and performance of AI models, especially in terms of time and space complexity.

Data Collection and Data Analysis

Cybersecurity incident data is gathered from diverse sources. Incident reports generated by organizations detail security events, breaches, and attempted attacks, providing a wealth of contextual information. Additionally, subscribing to threat intelligence feeds offers real-time updates on emerging threats, vulnerabilities, and indicators of compromise. Publicly available data, including open-source intelligence (OSINT), news articles, and government reports, supplements the collection process. Aggregating and processing this information is a critical step, involving the organization and structuring of data for subsequent analysis.

- **Cyber Harassment:** July-Dec 2018: 565 incidents Jan-Jun 2019: 784 incidents Increase: +219 incidents
Elaboration: Cyber harassment incidents increased by 219 from the second half of 2018 to the first half of 2019. This rise could be attributed to evolving online behaviors, increased social media usage, or changes in reporting mechanisms. Understanding the nature of these incidents and the platforms involved is essential for devising targeted prevention and response strategies.

- **Online Fraud:**
July-Dec 2018: 5789 incidents
Jan-Jun 2019: 5965 incidents
Increase: +180 incidents
Elaboration: The increase in online fraud incidents suggests a persistent threat landscape. Organizations and individuals need to stay vigilant against evolving fraud tactics. Analyzing the specific types of online fraud and the methods employed can guide the implementation of more effective cybersecurity measures and user awareness campaigns.

- **Spam:**
July-Dec 2018: 655 incidents
Jan-Jun 2019: 698 incidents
Increase: +44 incidents
Elaboration: While spam may seem less severe than some other cyber threats, the increase indicates a need for improved email filtering and user education. Organizations should assess the sources and content of spam to enhance email security measures and protect against potential phishing attacks.

- **Content-related Incidents:**
July-Dec 2018: 755 incidents
Jan-Jun 2019: 797 incidents
Increase: +41 incidents
Elaboration: Content-related incidents encompass a broad category, including issues like inappropriate content, copyright violations, or other content policy breaches. Understanding the specific nature of these incidents can guide content moderation efforts and ensure a safer online environment.

Role of Artificial Intelligence:

- **Pattern Recognition and Anomaly Detection:**
AI excels in identifying patterns and anomalies within large datasets. In cybersecurity, this capability allows AI systems to analyze historical incident data, recognizing patterns associated with known threats and detecting anomalies indicative of novel attack vectors.

- **Behavioral Analysis:**
Behavioral analysis, facilitated by AI, involves studying user activities and network traffic. By learning normal behavior, AI can identify deviations signaling potential security incidents, contributing to the detection of insider threats or advanced persistent threats (APTs).

- **Machine Learning for Threat Detection:**
Machine learning models are trained on extensive datasets to recognize malicious patterns and characteristics. These models can then operate in real-time, identifying and blocking potential threats based on learned patterns.

- **Natural Language Processing (NLP):**NLP enables the analysis of unstructured data, such as text from incident reports, forums, or social media. AI-driven NLP provides additional context and insights into emerging threats or vulnerabilities.

BENEFITS OF AI IN CYBERSECURITY

- **Unknown Threats:** A human individual may not be able to recognize all of a company's dangers. Every year, hackers carry out hundreds of millions of assaults for a variety of reasons. Unknown threats may do a lot of harm to the network. As attackers try new strategies, such as sophisticated social engineering and malware assaults, contemporary solutions are needed to protect against them. AI has shown to be one of the most successful technologies for spotting & preventing unanticipated threats from wrecking havoc on the company.
- **Better Vulnerability Management** Vulnerability management is essential to securing a company's network. As mentioned earlier, a median company deals with several threats daily. It must detect, establish and stop them to be safe. AI helps you assess systems faster than cyber security personel, there by increasing your downside determination ability manifold. That creates it potential to manage vulnerability and secure business systems in time.
- **Ai Authentication And Security** Most websites have a user account feature where one logs in to access services or buy products. Visitors are required to fill out sensitive information on some websites' contact forms. As a business, you must add an additional layer of protection because running such a site entails handling sensitive data and personal information. Your visitors' safety while using your network is guaranteed by the extra security layer. Every time a user tries to connect into their account, AI secures authentication.

CONCLUSION

Today, people are living in cyber world where total data or information is maintained in digital/online form. The information may be related to personal life, financial transactions, intellectual property or any other official information which is important in nature. The integration of AI technologies has yielded substantial achievements in bolstering the capabilities of cybersecurity defenses. From augmenting threat intelligence to enhancing anomaly detection and incident response, AI has demonstrated its prowess in navigating the complexities of modern cyber threats.

The future trajectory of AI in cybersecurity, it is imperative to consider the recommendations derived from this research. Interdisciplinary collaboration, continuous research, and the development of adaptive AI models are paramount. Ethical frameworks must evolve alongside technological advancements to ensure responsible and accountable use. The imperative for global cooperation in establishing regulatory standards becomes increasingly apparent, transcending geographical boundaries to fortify the collective defense against cyber threats

REFERENCES

1. J. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", The International Journal of FORENSIC COMPUTER SCIENCE, vol. 1, pp. 28-32, 2006
2. S. Adebukola, Onashoga, Akinwale O. Bamidele and A. Taofik, "A Simulated Multiagent- Based Architecture for Intrusion Detection System", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, vol. 2, no. 4, 2013
3. S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015
4. J.Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, vol. 8, no. 1, pp. 247-256, 2014
5. Cerli and D. Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", Global Journal of Pure and Applied Mathematics (GJPAM), vol. 11, no. 1, 2015
6. O. Oriola, A. Adeyemo and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme", African Journal of Computing & ICT, vol. 5, no. 2, 2012
7. S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 5, 24-26
8. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",RoEduNet International Conference 12th Edition: Networking in Education and Research, pp. 1-6, 26-28, 2013