International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-11, Issue-6; Jun, 2024
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.116.3

Improving Cyber Security: Artificial Intelligence's Ability to Detect and Stop Threats

Subha Laxmi[1,*], Satish Kumar[2]

[1]MTech Scholar – GITAM, Department of ECE, Kablana, Jhajjar, Haryana, India
[2]GITAM, Department of ECE, Kablana, Jhajjar, Haryana, India
*Corresponding Author : Laxmisubha990@gmail.com

Received: 29 Apr 2024,

Receive in revised form: 30 May 2024,

Accepted: 11 Jun 2024,

Available online: 17 Jun 2024

***Keywords*— Cyber Security, Artificial Intelligence, Threat identification, Predictive modeling, Machine learning**

***Abstract*—** *Artificial intelligence has become a crucial element of cyber security because of its capacity to assess security threats instantly and respond appropriately. Nowadays, AI plays a more significant role in identifying and thwarting attacks that keep companies innovative. The primary goals of artificial intelligence in cybersecurity are threat identification and mitigation. Artificial intelligence uses machine learning algorithms and sophisticated data analysis to identify patterns and abnormalities in user behavior and network traffic that can point to a possible cyberattack. Artificial Intelligence can help stop attacks by using predictive modeling. AI is also capable of anticipating dangers and preventing them by analyzing historical attacks and finding patterns. Automated incident response system creation is just another crucial cybersecurity use of artificial intelligence. These systems can assess data, spot possible threats, and then take action to lessen the impact of the attack by containing it or mitigating its effects. Artificial intelligence must be used by businesses in cybersecurity to safeguard their networks and sensitive data against ever-evolving online threats. Artificial intelligence (AI) is quickly emerging as a crucial tool for effective cybersecurity in today's digital environment due to its capacity to evaluate massive volumes of data in real-time and automate incident response. The importance of artificial intelligence (AI) in cybersecurity, particularly its applications in threat identification and defense.*

I. INTRODUCTION

In the battle against cybercrime, artificial intelligence is emerging as a significant technological tool. Artificial intelligence-based cybersecurity solutions can assist enterprises stay ahead of cyber-attacks by automating response actions, and detecting and preventing threats in real time (Srivastava et al., 2021).

Traditional security methods are no longer adequate to ward against sophisticated cyber threats since cybercrime has expanded quickly (Samiullah, 2019a). Because AI can evaluate and identify threats, forecast future assaults, and automate reaction measures, it is an essential tool for cybersecurity. Cybersecurity solutions powered by AI can be used.

Using machine learning and deep learning algorithms, a lot of data and information can be analyzed to find patterns and abnormalities that could be signs of possible cyber threats (Battelle et al., 2019a). These solutions are especially helpful in identifying new and developing threats that conventional signature-based methods might miss. AI can also detect patterns, quickly analyze massive amounts of data, and learn from past mistakes to foresee and stop attacks in the future. Artificial intelligence (AI)--

driven problem detection can quickly identify potential threats and reduce the amount of time needed to identify and resolve the issue.

The primary focus is on automating threat detection and response.

AI is always able to react to threats in real time, and automation can help speed up response times as well. By reducing the need for human analysts, this automation can also assist businesses in lowering their cybersecurity expenses (Xiaoguang et al., 2021). By locating weaknesses in various systems and networks, AI can assist enterprises in strengthening their security posture. AI can detect possible weak points in a network and provide ways to counteract threats by analyzing the network traffic (Sadiku et al., 2020a). Organizations that adopt this cybersecurity strategy can stop attacks in their tracks.

Businesses are increasingly depending on artificial intelligence in cybersecurity to secure their networks and sensitive data from ever-increasing cyber threats.

By employing AI to identify and stop assaults in real time, organizations can take preemptive measures to reduce the risk of data loss and disruption (Oku tan & Eyüpoglu, 2021).

The use of artificial intelligence in cybersecurity is crucial for the development of automated incident response systems.

These systems can assess the information, spot possible threats, and then take action to lessen the attack's impact by containing it or mitigating its effects. If attacks become widespread, this is crucial. It's possible that human help won't be able to react quickly enough. There are benefits and drawbacks to using AI in cybersecurity (Zhang, Hamadi, et al., 2022). Threat intelligence is the most crucial use of AI in cybersecurity. Massive volumes of data from several sources can be analyzed by AI to find patterns and trends that point to possible cyberthreats (Sahoo & Yadav, 2022). Artificial Intelligence (AI) can assist firms in staying ahead of cybercriminals by anticipating and averting future attacks by evaluating this data. Through the provision of up-to-date information on emerging threats, this threat intelligence can assist businesses in strengthening their incident response capabilities. AI can enhance cybersecurity by enhancing access control systems and authentication procedures (Abbas et al., 2019). Organizations can guarantee that only authorized users have access to their systems and networks by implementing AI-based biometric authentication solutions. Through the analysis of user behavior and the recognition of patterns that point to possible risks, these systems are also capable of detecting and stopping unwanted access attempts. By identifying and addressing vulnerabilities at the device level, AI can help improve end-point security (Zhang, Ning, et al., 2022).

II. TECHNIQUES OF ARTIFICIAL INTELLIGENCE REGARDING CYBERSECURITY

Cybersecurity has undergone a revolutionary change thanks to AI technology. These methods provide cybersecurity experts the ability to examine vast volumes of data, spot trends, and abnormalities, and recognize possible risks before they materialize into actual attacks (Thuraisingham, 2020). The AI methods listed below are frequently employed in cyber security.

Machine Learning

This kind of AI allows computers to learn from data without the need for explicit programming. In order to discover trends and identify potential risks, machine learning algorithms are trained on vast datasets of both benign and malicious traffic (Merat & Almuhtadi, 2015). Applications of machine learning include virus, anomaly, and network intrusion detection.

Natural Language Interpretation

It's a subset of artificial intelligence (AI) that lets computers comprehend and interpret human language. NLP is used in cybersecurity to look for possible vulnerabilities in unstructured data sources like online forums and social media feeds.

In-depth Learning

It is a branch of machine learning that makes use of deep neural networks to extract intricate patterns from data. It is employed in cybersecurity to carry out activities such as fraud, phishing, and virus detection.

Learning via Reinforcement

This subgroup of ML places a strong emphasis on judgment.

Systems can be trained to respond to attacks in cybersecurity by using reinforcement learning, which takes into account the circumstances and perceived threat level of each attack.

Computer Vision

It's an AI method that lets computers examine and interpret visual data. It is employed in cybersecurity for activities such as video monitoring and facial recognition.

Skillful Frameworks

These artificial intelligence (AI) systems imitate human decision-making abilities in a certain field. These systems are utilized in cybersecurity for activities including

vulnerability assessment and intrusion detection and response.

III. ARTIFICIAL INTELLIGENCE-BASED THREAT DETECTION

Be it homeland security, cybersecurity, or physical security. A vital part of maintaining the security of individuals and organizations is threat detection. Artificial intelligence technology advancements have made it easier to identify and eliminate risks in real-time (Shamiulla, 2019b). Threat detection systems based on artificial intelligence (AI) enable security systems to identify threats and hazards more quickly, accurately, and effectively. With the use of algorithms and machine learning approaches, AI-based threat detection systems may identify patterns in vast amounts of data that may indicate possible threats (G. A., 2022). A variety of data sources, including social media feeds, network traffic, and video surveillance footage, can be utilized to train AI systems to recognize and alert security professionals.

The algorithms are capable of learning from large data sets and identifying minute patterns thanks to the application of deep learning techniques.

This could imply that one of the most crucial elements of AI-based threat identification is potential hazards. Deep learning uses neural networks to mimic the way the human brain learns, enabling algorithms to improve in accuracy over time by identifying and assimilating new data points (Rehman, 2022). Thanks to AI-based threat detection, which is very good at identifying threats in real time, security teams can react quickly and prevent potential dangers from turning into big security events. These systems can detect and follow threats across several systems and networks because they can analyze data from multiple sources at once.

Threat detection systems that use artificial intelligence (AI) can identify a wide range of threats, depending on the data and algorithms that are used. For instance, these technologies are capable of identifying phishing schemes, malware, and other internet hazards (Kuzlu et al., 2021). In the context of physical security, artificial intelligence (AI) can identify questionable activities or behavior in video surveillance footage, such as theft or unlawful access. In homeland security, artificial intelligence (AI) can analyze social media feed data to find possible terrorist threats. The use of AI in danger detection has various benefits. Due to the effectiveness and precision of AI-based solutions, security personnel can quickly identify risks and take appropriate action. These systems' rapid mass data analysis capabilities make them ideal for evaluating data from multiple sources simultaneously. AI systems can also get more accurate over time by picking up new information and adjusting to it, which reduces the likelihood of false positives (Sadiku et al., 2020b).

IV. ARTIFICIAL INTELLIGENCE BASED CYBER SECURITY ASPECTS

Our civilization is evolving quickly as a result of computer technology advancements (Mehra & Badotra, 2021). The impact of this on people's daily routines and employment is substantial. Some of these technological advancements have made it feasible to create computers with cognitive functions like learning, decision-making, and problem-solving that are comparable to those of humans.AI is capable of analyzing vast volumes of data and applying intelligence to make decisions instantly. The application of AI techniques is beneficial to several technological and scientific domains (Achi et al., 2021). It is no secret that there is a lot of personal data on the Internet, which causes a lot of cybersecurity issues. First of all, manual analysis is nearly difficult due to the volume of data. Second, there might be risks related to AI or emerging risks. In addition, the high cost of employing experts drives up the cost of averting threats (Ansari et al., 2022). It also takes a great deal of time, money, and effort to design and implement the algorithms needed to recognize those threats.

One way to address those issues is to use AI-based methods. AI can analyze large amounts of data fast, accurately, and effectively

(Cyber_Security_Based_on_Artificial_Intelligence_for_Cyber-Physical_Systems, n.d.). Using threat history, an AI-based system can forecast future attacks that will resemble past ones, even if the patterns of those attacks differ. AI is able to manage enormous amounts of data, identify fresh, noteworthy variations in attacks, and continuously enhance the way its security system responds to dangers.

The use of AI in cybersecurity has transformed the conventional security strategy from reactive to proactive, helping to identify and mitigate threats in real-time (Rawat et al., 2022).

Here are a few cybersecurity techniques that use AI:

- Threat Identification and Evaluation

Large volumes of data can be automatically analyzed by AI-based threat detection systems to find possible security risks. Machine learning algorithms are able to recognize malicious code in network traffic and discover trends and anomalies in files and examine user conduct to identify any questionable conduct (Bishtawi & Alzubi, 2022).

- Fraud Identification

Massive data sets can be analyzed by AI-based fraud detection systems to find fraudulent activity or transactions. According to Benzaïd and Taleb (2020), these systems have the ability to recognize anomalous patterns, behaviors, and trends in financial transactions, which can aid in the prompt detection of fraud.

- Analytics of User and Entity Behavior

UEBA is an AI-based method that looks for unusual activity and behavior in user accounts and devices using machine learning algorithms. It can identify compromised accounts or malevolent insiders, which are difficult to find using conventional security techniques.

- Incident Response

Systems powered by AI can automate the reaction to cyberthreats, cutting down on the amount of time needed to counter an attack. These technologies are capable of analyzing data from multiple sources and giving the security team useful insights so they can act promptly and appropriately (Bhatele et al., 2019b).

- Virtual assistants and chatbots

Routine security chores, including account management and password resets, can be automated with the use of chatbots and virtual assistants driven by artificial intelligence. Additionally, they can offer users immediate support, enabling them to swiftly address security-related problems.

- Cybersecurity Intelligence

Massive volumes of data from several sources can be analyzed by AI-based threat intelligence systems to find new threats and vulnerabilities (Li, 2018). They have the ability to offer enterprises proactive protection against cyber threats by providing real-time threat intelligence.

V. DISCUSSION

Artificial intelligence has emerged as a key instrument in the cybersecurity space in recent years (Rekha et al., 2020). Due to the daily increase in the volume and complexity of cyber threats, organizations have begun utilizing AI-based systems for the detection and prevention of cyberattacks.

a) AI-powered threat detection

Threat detection is AI's main function in cybersecurity.

In the past, threat detection systems have mostly relied on signature-based techniques, which are limited to identifying known threats. However, because cyber threats are becoming more sophisticated, these measures are no longer as effective.

One of the most popular AI methods for threat detection is machine learning (Ghillani, 2022). Massive data sets can be analyzed by ML models, which can then be used to spot patterns that point to potential threats. The models are able to effectively identify possible threats since they are trained on datasets containing both benign and malicious traffic. ML models, for instance, are able to identify unusual network activity that can point to a possible hack. Another artificial intelligence method for danger detection is deep learning. Deep Learning models classify and analyze data using deep neural networks. These models may identify complex patterns and classify them as either positive or negative.

For example, deep learning models are capable of identifying and classifying phishing scams, malware, and other online dangers. Another AI technology used in threat detection is Natural Language Processing (NLP). To find possible risks, NLP algorithms can examine unstructured data sources like internet forums and social media feeds. The accuracy of threat detection can be increased by the algorithms' ability to extract information from text data (Alhayani et al., 2021).

b) AI-based threat prevention

AI can also be utilized for threat prevention in addition to danger detection. AI-based systems are able to recognize possible dangers and take preventative action before they have a chance to do any damage.

Here are some instances of how artificial intelligence is being used to counter threats:

1. Intrusion Prevention: Systems that employ artificial intelligence to prevent intrusions can identify and neutralize them before they have a chance to infiltrate the network.

2. Malware Prevention: AI-driven anti-malware programs are able to identify and stop malicious software from being installed.

3. Phishing Prevention: By examining emails and spotting questionable content, AI-based ant phishing systems may identify and stop phishing assaults.

4. Vulnerability Assessment: AI-based vulnerability assessment systems are capable of seeing possible network vulnerabilities and taking preventative action to lessen them.

AI-powered access control systems have the ability to recognize possible hazards and prevent unauthorized individuals from entering.

VI. CONCLUSION

The role that artificial intelligence will play in cybersecurity is rapidly evolving and growing in significance.

Because cyber threats are so sophisticated and dynamic, traditional approaches to threat detection and prevention are no longer sufficient. Artificial intelligence (AI) technologies offer sophisticated and innovative ways to thwart cyberattacks. Artificial intelligence (AI)-based systems use techniques including machine learning, deep learning, natural language processing, predictive analytics, and behavioral analytics to detect and block cyber threats.

These systems are capable of analyzing massive amounts of data, identifying patterns, and making predictions that are not possible with traditional methods.

Furthermore, because AI-based systems can recognize and neutralize both known and unknown threats, they are a helpful tool for companies looking to stay ahead of cyberattacks. Because they may be used for access control, vulnerability assessment, intrusion prevention, malware protection, and phishing prevention, these systems offer an all-in-one cybersecurity solution.

As technology advances, so too will the use of AI in cybersecurity. Companies will need to adjust and use these state-of-the-art solutions if they want to ensure that their systems are protected from cyberattacks. AI is expected to become a critical component of cybersecurity in the near future, and businesses that invest in these technologies will have enhanced defenses against cyberattacks.

REFERENCES

[1] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. Scientometrics, 121(2), 1189– 1211. https://doi.org/10.1007/s11192-019-03222-9

[2] Achi, A., Kuwunidi Job, G., Shittu, F., Baba Atiku, S., Unimke Aaron, A., & Zahraddeen Yakubu, I. (2021). SEE PROFILE Survey On The Applications Of Artificial Intelligence In Cyber Security. Survey On The Applications Of Artificial Intelligence In Cyber Security Article in International Journal of Scientific & Technology Research. www.ijstr.org

[3] Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2021.02.531

[4] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. IJARCCE, 11(9). https://doi.org/10.17148/ijarcce.2022.11912

[5] Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? IEEE Network, 34(6), 140–147. https://doi.org/10.1109/MNET.011.2000088

[6] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019a). The Role of Artificial Intelligence in Cyber Security (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

[7] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019b). The Role of Artificial Intelligence in Cyber Security (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

[8] Bishtawi, T., & Alzubi, R. (2022). Cyber Security of Mobile Applications Using Artificial Intelligence. 1st International Engineering Conference on Electrical, Energy, and Artificial Intelligence, EICEEAI 2022. https://doi.org/10.1109/EICEEAI56378.2022.10050484

[9] Cyber_Security_Based_on_Artificial_Intelligence_for_Cyber-Physical_Systems. (n.d.).

[10] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920. https://doi.org/10.3390/electronics12081920

[11] G. A., S. (2022). The Review of Artificial Intelligence in Cyber Security. International Journal for Research in Applied Science and Engineering Technology, 10(1), 1461–1468. https://doi.org/10.22214/ijraset.2022.40072

[12] Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. American Journal of Artificial Intelligence, x, No. x, x–x. https://doi.org/10.22541/au 166379475.54266021/v1

[13] Harel, Y., Gal, I. Ben, & Elovici, Y. (2017a). Cyber security and the role of intelligent systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology, 8(4). https://doi.org/10.1145/3057729

[14] Harel, Y., Gal, I. Ben, & Elovici, Y. (2017b). Cyber security and the role of intelligent systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology, 8(4). https://doi.org/10.1145/3057729

[15] Jenis Nilkanth Welukar, & Gagan Prashant Bajoria. (2021). Artificial Intelligence in Cyber Security - A Review International Journal of Scientific Research in Science and Technology, 488–491. https://doi.org/10.32628/ijsrst218675

[16] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1(1). https://doi.org/10.1007/s43926-020-00001-4

[17] Li, J. hua. (2018). Cyber security meets artificial intelligence: a survey. In Frontiers of Information Technology and Electronic Engineering (Vol. 19, Issue 12, pp. 1462–1474). Zhejiang University. https://doi.org/10.1631/FITEE.1800573

[18] Mehra, A., & Badotra, S. (2021). Artificial Intelligence Enabled Cyber Security. Proceedings of IEEE International Conference on Signal Processing, Computing and Control, 2021-October, 572–575. https://doi.org/10.1109/ISPCC53510.2021.9609376

[19] Merat, S., & Almuhtadi, W. (2015). Artificial intelligence application for improving cyber-security

acquirement. Canadian Conference on Electrical and Computer Engineering, 2015- June (June), 1445–1450. https://doi.org/10.1109/CCECE.2015.7129493

[20] Okutan, A., & Eyüpoglu, C. (2021). A Review on Artificial Intelligence and Cyber Security. Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021, 304–309. https://doi.org/10.1109/UBMK52708.2021.9558949

[21] Rawat, B. S., Gangodkar, D., Talukdar, V., Saxena, K., Kaur, C., & Singh, S. P. (2022). The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 247–250. https://doi.org/10.1109/IC3I56241.2022.10072877

[22] Rehman, S. F. U. (2022). Practical Implementation of Artificial Intelligence in Cybersecurity – A Study. IJARCCE, 11(11). https://doi.org/10.17148/ijarcce.2022.111103

[23] Rekha, G., Malik, S., Tyagi, A. K., & Nair, M. M. (2020). Intrusion detection in cyber security: Role of machine learning and data mining in cyber security. Advances in Science, Technology and Engineering Systems, 5(3), 72–81. https://doi.org/10.25046/aj050310

[24] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020a). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

[25] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020b). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

[26] Sahoo, B. M., & Yadav, S. A. (Eds.). (2022). Information Security Practices for the Internet of Things, 5G, and Next- Generation Wireless Networks. IGI Global. https://doi.org/10.4018/978-1-6684-3921-0

[27] Shamiulla, A. M. (2019a). Role of artificial intelligence in cyber security. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119