Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1367–1375
DOI : 10.47974/JDMSC-1991

Applications of artificial intelligence in cyber security

Pragya Vaishnav [†]
Linesh Raja [§]
Poonam Singh *
Department of Computer Applications
Manipal University Jaipur
Jaipur
Rajasthan
India

Swapnali Tandel [‡]
Department of B.Sc. Computer Science and Information Technology
Nagindas Khandwala College
Malad
Mumbai
Maharashtra
India

Abstract

Artificial Intelligence (AI) in cyber security can assist businesses in recognising and understanding problems. Based on earlier research, this study intends to give a current overview of AI's application in cyber security and assess the possibility of improving cyber security through greater AI use. Nonetheless, it's critical to take into account the drawbacks and difficulties of using AI to cybersecurity and to combine it with other cybersecurity measures.

Subject Classification: *68T35.*

Keywords: *Cyber security, Artificial intelligence, Expert systems, Neural nets, Intelligence agent.*

[†] *E-mail:* **pragya.vaishnav23@gmail.com**
[§] *E-mail:* **lineshraja@gmail.com**
* *E-mail:* **poonam.rani4@gmail.com (Corresponding Author)**
[‡] *E-mail:* **swapnali.tandel22@gmail.com**

1. Introduction

Artificial intelligence (AI) is the modelling of human intellectual functions by computers, especially computer systems [1]. To make our computers safer and more resistant to these types of hackers, cyber security is merely a moral endeavour [2-5]. Artificial Intelligence (AI) in cyber security provides insights that help businesses understand problems. These disclosures can help businesses adhere to security best practices and expedite response times. These disclosures could be about network security, threat hunting, or vulnerability management, for example, researchers have been attempting to incorporate machine learning into cybersecurity solutions since the late 1980s, but their progress has been sluggish. Intrusion detection systems (IDS) were initially created by researchers in 1987.

This study's primary goal is to present a current overview of AI applications in cyber security based on prior research and evaluate the possibility of enhancing cyber security capabilities [6-10].

2. Potential Cyber Security Solutions Utilizing AI

This research offers a current summary of a number of AI-powered prospective cyber security solutions, including malware categorization, network information sharing, anomalous traffic identification, tracking dangerous activities, and user access verification [9] [11-12].

2.1 *Classification of Malware*

Any software intended to damage or take advantage of computer systems is referred to as malware, short for malicious software. It can manifest itself in a variety of ways, such as worms, trojans, ransomware, and viruses. Due to its ability to destroy systems, steal confidential data, and interfere with daily operations, malware poses a serious risk to both persons and organisations [13-16].

The application of AI to malware classification is one possible defence against this menace. Malware can be analysed and categorised by AI using a variety of criteria, including code, behaviour, and impact. This can make it easier and more efficient for cybersecurity experts to recognise and eliminate threats. There are various methods for classifying malware with artificial intelligence. One method is to categorise software as benign or malicious by analysing its code using machine learning methods. This can be achieved by teaching the algorithm on a sizable dataset of software that

is both benign and malicious, enabling it to discover the traits that tell each apart.

Using artificial intelligence (AI) to examine software behaviour is an additional strategy. This can be accomplished by launching the programme in a virtual environment and watching what happens. The programme can then be categorised by AI according to whether its behaviour is characteristic of malicious or benign software. AI is also capable of evaluating the effects of infection on a system. Analysing the malware's impact on the system's functionality, stability, and security may be part of this. AI can categorise the infection according to its possible impact to the system based on this study [9].

A further study examined the application of a hybrid AI model for malware classification and was published in the journal "Expert Systems with Applications". With the use of artificial neural networks and rule-based algorithms, the model successfully identified and categorised different kinds of malware [6].

2.2 *Information Sharing*

Information sharing over networks is a widespread and crucial component of many businesses and organisations in the modern digital age. But with greater connection comes a higher chance of data breaches and cyberattacks.

The application of AI to networked information exchange is one possible countermeasure to this issue. Artificial Intelligence has the ability to examine and track the information that moves through a network, identifying and stopping illegal access or alteration. This can support preserving the network's integrity and safeguarding sensitive data. AI can be applied in a variety of ways to networked information sharing. Using machine learning algorithms to examine network data and spot trends that can point to a potential cyberattack is one method. Analysing the traffic's origin and destination as well as the type and structure of the data being transferred can all be part of this.

Utilising AI to keep an eye on network resource access is an additional strategy. This may entail tracking users' activities, identifying and authenticating them, and looking for any unusual or suspect activity. AI is also capable of enforcing network security regulations.

Numerous studies have been done on the application of AI to information sharing in the context of cyber security. One such study looked at the application of a hybrid AI model for cyberattack detection

and prevention, and it was published in the journal "Expert Systems with Applications." The algorithm was able to accurately identify and categorise a variety of cyberattacks by combining artificial neural networks and rule-based systems [8].

2.3. *Unusual Traffic Identification*

Any divergence from the regular flow of data on a network is referred to as unusual traffic. This can be a sign of a distributed denial of service (DDoS) attack or other type of malware infestation. Maintaining network security requires recognising and responding to anomalous traffic.

The application of AI to the identification of anomalous traffic is one possible way to address this problem. AI is able to examine network data and spot trends that can point to a potential cyberattack. Analysing the traffic's origin and destination as well as the composition and format of the data being sent may be necessary to achieve this.

There are various methods for using AI to the identification of anomalous traffic. Using machine learning algorithms to examine network data and spot patterns indicative of cyberattacks is one method. This can be achieved by teaching the algorithm on a sizable dataset that includes both typical and anomalous traffic, enabling it to pick up on the traits that set each apart.

Using AI to track traffic on a network in real time is an additional strategy. This may entail installing sensors or other monitoring tools that track traffic data continually and notify cybersecurity experts of any anomalies from the usual.

Numerous studies have been done on the application of AI in the context of cyber security for the identification of atypical traffic. One such study looked at the application of machine learning algorithms for identifying and categorising anomalous traffic patterns, and it was published in the "Journal of Network and Computer Applications."

An additional investigation into the application of a hybrid AI model for odd traffic recognition was published in the journal "Expert Systems with Applications". The programme was able to precisely recognise and categorise a variety of odd traffic kinds by combining artificial neural networks with rule-based systems [3].

2.4 *Unsafe Activity Tracking*

Any activity that could jeopardise a system or network's security is considered unsafe. Malware infections, illegal access, and other

cyberattacks can fall under this category. An essential component of keeping up cyber security is monitoring and responding to dangerous activities.

The application of AI to the tracking of risky behaviour is one possible answer to this problem. Artificial Intelligence has the ability to examine user and system behaviour and spot trends that can point to a potential cyberattack. This may entail examining user behaviour, including the files they access and the websites they visit, in addition to system stability and performance assessments.

There are various methods for using AI to the tracking of risky behaviour. Using machine learning algorithms to examine system and user behaviour and spot patterns that are indicative of cyberattacks is one method. This can be achieved by teaching the algorithm on a sizable dataset that includes both safe and risky activities, enabling it to pick up on the traits that set one apart from the other.

Numerous studies have been done on the application of AI in the context of cyber security to track risky activity. Within the "Journal of Network and Computer Applications," one such study looked at the application of machine learning algorithms to the identification and categorization of risky behaviour. In comparison to conventional rule-based methods, the study indicated that the usage of AI was able to greatly enhance the accuracy of tracking risky activity [10].

A hybrid AI model was investigated in a different study that was published in the journal "Expert Systems with Applications" to track dangerous activity. The programme successfully identified and classified different kinds of dangerous activity by combining artificial neural networks and rule-based systems [11].

2.5 *Unusual Traffic Identification*

Verifying a user's identity when they want to access a system or network is known as user access verification. This is crucial for preserving cyber security since it guards sensitive information and stops illegal access.

The application of AI to user access verification is one possible remedy for this problem. Artificial Intelligence has the ability to examine user attributes, including past login history, behaviour on the platform, and additional data, in order to verify a user's identity. This may entail analysing behavioural patterns and spotting anomalies that can point to a potential cyberattack using machine learning techniques.

One potential solution to this issue is the use of AI in user access verification. Artificial intelligence is capable of analysing user characteristics, such as previous login history, platform behaviour, and extra data, to confirm an individual's identification. This can involve applying machine learning techniques to analyse behavioural patterns and identify abnormalities that would indicate a possible cyberattack.

Utilising AI to examine user behaviour while they engage with the system is an additional strategy. This may entail monitoring their activities, including the files they open and the websites they visit, and utilising machine learning algorithms to spot behavioural patterns characteristic of a genuine user.

Artificial intelligence (AI) can also be used to identify and stop cyberattacks that entail pretending to be authentic users. In order to do this, it may be necessary to examine user attributes and look for any variations from the norm, such as odd login times or locations [16].

Numerous studies on the application of AI to user access verification in cyber security contexts have been carried out. Within the "Journal of Network and Computer Applications," one such study looked at the application of machine learning algorithms to the identification and categorization of anomalous user behaviour. The study discovered that, in comparison to conventional rule-based methods, the application of AI was able to greatly increase the accuracy of user access verification [4].

An additional investigation into the application of a hybrid AI model for user access verification was published in the journal "Expert Systems with Applications". The model successfully recognised and categorised anomalous user behaviour and activity by fusing artificial neural networks and rule-based systems [11].

3. Results

The application of AI to cyber security solutions has a number of possible advantages. Its ability to analyse massive volumes of data fast and reliably is one advantage. This can lower the risk of unauthorised access and data breaches by enabling organisations to authenticate user identities more quickly and effectively.

The ability of AI to continuously learn and adapt is another advantage. It can get more adept at recognising and stopping cyberattacks as well as authentic user identification as it becomes more exposed to data. This can assist it in keeping abreast of the most recent threats and bolster its defences more successfully.

The application of AI to cyber security solutions is not without its difficulties. One difficulty is that accurate algorithm training necessitates a substantial volume of data. Obtaining this can be challenging, particularly for uncommon or unique forms of cyberattacks.

4. Discussion

Even though this research show how AI can be used for cyber security, there is still room for development. The requirement for massive volumes of data to train machine learning models is one possible problem, which can be difficult in the quick-changing and dynamic field of cyber security.

All things considered, there is a lot of promise for using AI to verify user access in the context of cyber security. Enhancing the efficacy and efficiency of user behaviour analysis and access verification, as well as improving network security overall, is feasible with the creation and improvement of machine learning models and techniques. To fully realise the potential of AI in this context, however, more research and development in this field are required as there is still room for improvement.

5. Conclusion

This study evaluated the possibilities for enhancing cyber security capabilities by advocating that the intelligence of security systems be enhanced more quickly. It also offered an up-to-date review of AI applications in cyber security based on earlier research. Drawing from the aforementioned study, it is imperative to thoroughly examine the limitations and challenges associated with utilising AI in this particular scenario, and to integrate it with extant cybersecurity measures. Research on AI's use to cyber security is still ongoing. The creation of more sophisticated machine learning algorithms that can more precisely identify and categorise cyberthreats need additional study to be effective.

References

[1] A. Bécue, I. Praça, and J. Gama, "Artificial Intelligence, cyber-threats and Industry 4.0: Challenges and opportunities," *Artificial Intelligence Review*, vol. 54, no. 5, pp. 3849–3886 (2021).

[2] A. Chakraborty, A. Biswas, and A. Khan, "Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation" [Online]. Available: https://arxiv.org/pdf/2209.13454.pdf.

[3] C. Islam, M. A. Babar, R. Croft, and H. Janicke, "SmartValidator: A framework for automatic identification and classification of cyber threat data," *Journal of Network and Computer Applications*, vol. 202, p. 103370, Jun. (2022), doi: 10.1016/j.jnca.2022.103370.

[4] D. A. Shamiulla*, "Role of artificial intelligence in cyber security," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 4628–4630 (2019).

[5] D. Gibert, C. Mateu, and J. Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications,* vol. 153, p. 102526 (2020).

[6] D. Gibert, J. Planes, C. Mateu, and Q. Le, "Fusing feature engineering and Deep Learning: A Case Study for malware classification," *Expert Systems with Applications,* vol. 207, p. 117957 (2022).

[7] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "Distiller: Encrypted traffic classification via Multimodal Multitask Deep Learning," *Journal of Network and Computer Applications*, vol. 183-184, p. 102985 (2021).

[8] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," *Expert Systems with Applications,* vol. 37, no. 9, pp. 6225–6232, Sep. (2010), doi: 10.1016/j.eswa.2010.02.102.

[9] J.-hua Li, "Cyber Security Meets Artificial Intelligence: A survey," *Frontiers of Information Technology & Electronic Engineering,* vol. 19, no. 12, pp. 1462–1474 (2018).

[10] L. F. Carvalho, T. Abrão, L. de Mendes, and M. L. Proença, "An ecosystem for anomaly detection and mitigation in software-defined networking," *Expert Systems with Applications*, vol. 104, pp. 121–133 (2018).

[11] M. Abdullahi et al., "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, Jan. (2022), doi: 10.3390/electronics11020198.

[12] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[13] N. N. Abbas, T. Ahmed, S. H. Shah, M. Omar, and H. W. Park, "Investigating the applications of Artificial Intelligence in cyber security," Scientometrics, vol. 121, no. 2, pp. 1189–1211 (2019).

[14] R. Trifonov, O. Nakov, and V. Mladenov, "Artificial Intelligence in cyber threats intelligence," 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), (2018).

[15] Kumar, Ankit, et al. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 499-507 (2019).

[16] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, "Artificial Intelligence in cyber security: Research advances, challenges, and opportunities," *Artificial Intelligence Review*, vol. 55, no. 2, pp. 1029–1053 (2021).