# Artificial Intelligence (AI) Applications in Cyber Security

**Research** · January 2023

# Artificial Intelligence (AI) Applications in Cyber Security

Nadide Beyza Dokur
Computer Engineering, MEF University, Istanbul, Turkey

## Abstract

Artificial Intelligence (AI) in cyber security can help companies understand and comprehending issues. This research aims to provide a current overview of AI's use in cyber security based on previous studies and to evaluate the potential for enhancing cyber security through increased use of AI. However, it is important to consider the limitations and challenges of using AI in cyber security and to use it alongside other cybersecurity measures.

**Keywords:** cyber security, artificial intelligence, artificial intelligence applications, machine learning, cyber security systems

## Introduction

The modeling of human intellectual functions by machines, particularly computer systems, is known as artificial intelligence (AI) [17]. Cyber security is just a moral practice that aims to make our computers safer and protected from such hackers [18]. AI in cyber security offers insights that support companies in comprehending issues. These revelations can speed up reaction times and help companies stick to security best practices. For instance, these disclosures may relate to vulnerability management, threat hunting, and network security [9]. The brain of AI is machine learning (ML) [20]. In cybersecurity, machine learning algorithms can automatically find and evaluate security incidents. Since the late 1980s, researchers have attempted to integrate ML in cybersecurity solutions, but progress has been gradual. Researchers first developed intrusion detection (IDS) systems in 1987. DARPA (the government organization that developed the Internet) issued a request for research on ML techniques for security based on unsupervised learning in the period between 1998 and 1999. DARPA also published benchmark sets. Unfortunately, only a small percentage of the findings were useful, and even fewer items reached

the operational level. Following the year 2000, programmers and academics started developing supervised learning-based spam, phishing, and URL screening systems. Since years, supervised ML has been used to generate anti-virus signatures with success, and in 2012[19]. The main purpose of this study is to provide an up-to-date overview of AI applications in cyber security according to previous research and assesses the potential for improving cyber security capabilities by recommending that security systems' intelligence be increased more quickly.

**Potential Cyber Security Solutions Utilizing AI**

This study provides an up-to-date overview of several potential cyber security solutions that utilize AI, based on malware classification, information sharing on a network, unusual traffic identification, unsafe activity tracking, and user access verification [9][16].

1. **Malware Classification**

Malware, short for malicious software, refers to any software designed to harm or exploit computer systems. It can take many forms, including viruses, worms, trojans, ransomware, and more. Malware is a significant threat to individuals and organizations, as it can cause damage, steal sensitive information, and disrupt operations.

One potential solution to this threat is the use of AI in malware classification. AI can analyze and classify malware based on various features, such as code, behavior, and impact. This can help cybersecurity professionals identify and neutralize threats more efficiently and effectively.

There are several approaches to malware classification using AI. One approach is to use machine learning algorithms to analyze the code of a piece of software and classify it as malware or benign. This can be done by training the algorithm on a large dataset of both malicious and benign software, allowing it to learn the characteristics that distinguish one from the other.

Another approach is to use AI to analyze the behavior of a piece of software. This can be done by running the software in a virtual environment and observing its actions. AI can then classify the software based on whether its behavior is typical of malware or benign software.

AI can also be used to assess the impact of malware on a system. This can involve analyzing the effects of the malware on the system's performance, stability, and security. Based on this analysis, AI can classify the malware based on its potential harm to the system [9].

There have been a number of studies conducted on the use of AI for malware classification in the context of cyber security. One such study, published in the "Journal of Network and Computer Applications," examined the use of machine learning algorithms for detecting and classifying malware. The study found that the use of AI was able to significantly improve the accuracy of malware classification, compared to traditional rule-based approaches [5].

Another study, published in the "Expert Systems with Applications" journal, explored the use of a hybrid AI model for malware classification. The model combined both artificial neural networks and rule-based systems, and was able to effectively identify and classify various types of malware [6].

## 2. Information Sharing on A Network

In today's digital age, information sharing on networks is a common and essential part of many businesses and organizations. However, this increased connectivity also brings increased risk of cyber attacks and data breaches.

One potential solution to this risk is the use of AI in information sharing on networks. AI can analyze and monitor the flow of information on a network, detecting and preventing unauthorized access or manipulation. This can help protect sensitive data and maintain the integrity of the network.

There are several approaches to using AI in information sharing on a network. One approach is to use machine learning algorithms to analyze network traffic and identify patterns that may indicate an attempted cyber attack. This can involve analyzing the source and destination of the traffic, as well as the content and structure of the data being transmitted.

Another approach is to use AI to monitor access to network resources. This can involve identifying and authenticating users, as well as tracking their actions and detecting any anomalies or suspicious activity.

AI can also be used to enforce security policies on a network. This can involve setting rules for access to certain resources and automatically enforcing those rules based on the actions of users [16].

There have been a number of studies conducted on the use of AI for information sharing in the realm of cyber security. One such study, published in the journal "Expert Systems with Applications," examined the use of a hybrid AI model for detecting and preventing cyber attacks. The model combined both artificial neural networks and rule-based systems, and was able to identify and classify various types of cyber attacks with a high degree of accuracy [8].

Another study, published in the "Journal of Network and Computer Applications," focused on using AI to improve the efficiency and effectiveness of information sharing in the context of incident response. The researchers developed a framework that utilized machine learning algorithms to analyze and prioritize incoming information, allowing incident responders to more quickly and effectively address potential threats [5].

### 3. Unusual Traffic Identification

Unusual traffic refers to any deviation from the normal flow of data on a network. This can be an indication of a cyber attack, such as a malware infection or a distributed denial of service (DDoS) attack. Identifying and addressing unusual traffic is an important part of maintaining network security.

One potential solution to this challenge is the use of AI in unusual traffic identification. AI can analyze network traffic and identify patterns that may indicate an attempted cyber attack. This can involve analyzing the source and destination of the traffic, as well as the content and structure of the data being transmitted.

There are several approaches to using AI in unusual traffic identification. One approach is to use machine learning algorithms to analyze network traffic and identify patterns that are typical of cyber attacks. This can be done by training the algorithm on a large dataset of both normal and unusual traffic, allowing it to learn the characteristics that distinguish one from the other.

Another approach is to use AI to monitor the flow of traffic on a network in real-time. This can involve setting up sensors or other monitoring devices that continuously collect data on the traffic and alert cybersecurity professionals to any deviations from the normal pattern.

AI can also be used to prioritize the response to unusual traffic. This can involve ranking the potential threats based on their likelihood and impact, and directing resources towards the most serious threats first [16].

There have been a number of studies conducted on the use of AI for unusual traffic identification in the context of cyber security. One such study, published in the "Journal of Network and Computer Applications," examined the use of machine learning algorithms for detecting and classifying unusual traffic patterns. The study found that the use of AI was able to significantly improve the accuracy of unusual traffic identification, compared to traditional rule-based approaches [7].

Another study, published in the "Expert Systems with Applications" journal, explored the use of a hybrid AI model for unusual traffic identification. The model combined both artificial neural networks and rule-based systems, and was able to effectively identify and classify various types of unusual traffic [3].

### 4. Unsafe Activity Tracking

Unsafe activity refers to any actions that may compromise the security of a system or network. This can include malware infections, unauthorized access, and other types of cyber attacks. Tracking and addressing unsafe activity is an important part of maintaining cyber security.

One potential solution to this challenge is the use of AI in unsafe activity tracking. AI can analyze the behavior of users and systems and identify patterns that may indicate an attempted cyber attack. This can involve analyzing the actions of users, such as the files they access and the websites they visit, as well as the performance and stability of systems.

There are several approaches to using AI in unsafe activity tracking. One approach is to use machine learning algorithms to analyze user and system behavior and identify patterns that are typical of cyber attacks. This can be done by training the algorithm on a large dataset of both

normal and unsafe activity, allowing it to learn the characteristics that distinguish one from the other.

Another approach is to use AI to monitor user and system behavior in real-time. This can involve setting up sensors or other monitoring devices that continuously collect data on the activity and alert cybersecurity professionals to any deviations from the normal pattern.

AI can also be used to prioritize the response to unsafe activity. This can involve ranking the potential threats based on their likelihood and impact, and directing resources towards the most serious threats first [16].

There have been a number of studies conducted on the use of AI for unsafe activity tracking in the context of cyber security. One such study, published in the "Journal of Network and Computer Applications," examined the use of machine learning algorithms for detecting and classifying unsafe activity. The study found that the use of AI was able to significantly improve the accuracy of unsafe activity tracking, compared to traditional rule-based approaches [10].

Another study, published in the "Expert Systems with Applications" journal, explored the use of a hybrid AI model for unsafe activity tracking. The model combined both artificial neural networks and rule-based systems, and was able to effectively identify and classify various types of unsafe activity [11].

### 5. User Access Verification

User access verification refers to the process of verifying the identity of users who are attempting to access a system or network. This is an important part of maintaining cyber security, as it helps prevent unauthorized access and protect sensitive data.

One potential solution to this challenge is the use of AI in user access verification. AI can analyze the characteristics of users, such as their login history, their actions on the system, and other factors, to determine whether they are who they claim to be. This can involve using machine learning algorithms to analyze patterns of behavior and identify anomalies that may indicate an attempted cyber attack.

There are several approaches to using AI in user access verification. One approach is to use biometric data, such as fingerprints or facial recognition, to authenticate users. This can involve setting up sensors or other devices that collect this data and use it to verify the identity of users.

Another approach is to use AI to analyze the behavior of users as they interact with the system. This can involve tracking their actions, such as the files they access and the websites they visit, and using machine learning algorithms to identify patterns of behavior that are typical of a legitimate user.

AI can also be used to detect and prevent cyber attacks that involve the impersonation of legitimate users. This can involve analyzing the characteristics of users and detecting any deviations from the normal pattern, such as unusual login times or locations [16].

There have been a number of studies conducted on the use of AI for user access verification in the context of cyber security. One such study, published in the "Journal of Network and Computer Applications," examined the use of machine learning algorithms for detecting and classifying unusual user behavior. The study found that the use of AI was able to significantly improve the accuracy of user access verification, compared to traditional rule-based approaches [4].

Another study, published in the "Expert Systems with Applications" journal, explored the use of a hybrid AI model for user access verification. The model combined both artificial neural networks and rule-based systems, and was able to effectively identify and classify unusual user behavior and activity [11].

**Result**

There are several potential benefits to using AI in cyber security solutions. One benefit is that it can process large amounts of data quickly and accurately. This can allow organizations to verify the identity of users more efficiently and effectively, reducing the risk of unauthorized access and data breaches.

Another benefit is that AI can continuously learn and adapt. As it is exposed to more data, it can improve its ability to identify legitimate users and detect and prevent cyber attacks. This can help it stay up-to-date with the latest threats and more effectively protect against them.

There are also some challenges to using AI in cyber security solutions. One challenge is that it requires a large amount of data to train the algorithms accurately. This can be difficult to obtain, especially for rare or novel types of cyber attacks.

Another challenge is that AI can sometimes make mistakes, particularly when it is exposed to data that is significantly different from the data it was trained on. This can lead to false positives or false negatives, which can have serious consequences in the cybersecurity context.

**Discussion**

While these studies demonstrate the potential of AI for cyber security purposes, there are still areas for improvement. One potential issue is the need for large amounts of data to train machine learning models, which can be a challenge in the fast-paced and constantly-evolving world of cyber security.

Additionally, there is a need for further research and development in the use of AI for real-time user behavior analysis and access verification. As cyber threats continue to evolve and become more sophisticated, the ability to quickly and accurately verify user access is crucial.

Overall, the use of AI for user access verification in the context of cyber security holds significant potential. Through the development and refinement of machine learning models and approaches, it is possible to enhance the efficiency and effectiveness of user behavior analysis and access verification, and improve overall security on a network. However, there is still room for improvement and continued research and development in this area is necessary to fully realize the potential of AI in this context.

**Conclusion**

This study provided an up-to-date overview of AI applications in cyber security according to previous research and assesses the potential for improving cyber security capabilities by recommending that security systems' intelligence be increased more quickly. Based on the

analysis above, it's crucial to carefully analyze the restrictions and difficulties of employing AI in this situation and to combine them with existing cybersecurity safeguards. There is ongoing research into the use of AI in cyber security. Further research needed to work is the development of more advanced machine learning algorithms that can more accurately identify and classify cyber threats.

**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. [Accessed: Jan. 02, 2023]

[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] “Multidisciplinary field that encompasses,” *International Journal of Cyber Criminology*. [Online]. Available: https://www.cybercrimejournal.com/. [Accessed: 02-Jan-2023].

[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] S. Dilek, H. Cakır, and M. Aydın, “Applications of artificial intelligence techniques to Combating Cyber Crimes: A Review,” *International Journal of Artificial Intelligence & Applications*, vol. 6, no. 1, pp. 21–39, 2015.

[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.

[17] Wikipedia Contributors, “Artificial intelligence,” *Wikipedia*, Feb. 18, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Artificial_intelligence

[18] Wikipedia Contributors, “Cyber security,” *Wikipedia*, Apr. 29, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Machine_learning

[19] Wikipedia Contributors, “Internet,” *Wikipedia*, Dec. 21, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Internet

[20] Wikipedia Contributors, “Machine learning,” *Wikipedia*, Apr. 29, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Machine_learning