BOHR International Journal of Engineering
2022, Vol. 1, No. 1, pp. 52–56
DOI: 10.54646/bije.2022.10
www.bohrpub.com

REVIEW

A review: Artificial intelligence and expert systems for cyber security

Patil Rushikesh*

Department of Mechatronics Engineering, Chandigarh University, Punjab, India

***Correspondence:**
Patil Rushikesh,
rishipatil7007@gmail.com

Received: 22 October 2022; **Accepted:** 05 November 2022; **Published:** 25 November 2022

Artificial intelligence (AI) and expert systems are essential and vital tools to counter potentially dangerous threats in cyber security. The protection of data requires skilled cyber security technicians for various types of roles. The essential role of an expert system is to monitor the threats and assist the technician to strengthen security. The system uses various datasets like a machine and deep learning as well as reinforced learning in order to make intelligent decisions. The Internet of Things (IoT) is one of the major concerns for cyber security because it is potentially the second most likely vulnerable link in the cyber security environment because an attacker can easily gain access to the system by breaching any IoT device that is connected to the system. Still human is the strongest and potentially the weakest link in the cyber security environment. This review intends to present AI and expert systems for cyber security.

Keywords: cyber security, artificial intelligence, machine learning, deep learning, Internet of Things (IoT)

Introduction

Cyber security is the most challenging job for any cyber forensic expert and engineer working in the field around the world. The protection of data and systems requires highly skilled cyber security experts for different roles (1). The essential function of cyber security is to detect unauthorized activities in the system environment. Any malicious activity in the system environment can be raised as a potential threat, which requires the immediate attention of the experts. An intrusion detection system (IDS) is usually used to alert the protectors when any malicious activity takes place within the system environment (2).

Numerous solutions are being developed to protect against vulnerabilities and attacks, despite, it is becoming exponentially challenging to protect the system environment and data in the continuously changing virtual world. Implementation of continuous protection requires adjustment as per the changing environment. Artificial intelligence (AI) is becoming an important asset in order to make intelligent decisions in a short time (3). The Internet of Things (IoT) is reducing human effort to a massive extent but cyber security concerns are increasing exponentially along with it because anything that is connected to the Internet is a potential vulnerability and a concern for cyber security (4). The need for an expert system with required solutions is essential to defend the network system against cyber attacks and to increase the robustness of the system (Da, 2021).

Internet of Things (IoT) devices require special attention for protection from cyber attacks and other vulnerabilities; hence, AI technics would be a solution to the problem. AI systems are widely used for monitoring IoT devices to enhance security (5). AI is an essential tool, which is able to handle a massive amount of data with speed and precision. Expert systems are an essential AI tool. An associate skilled system is an example of an expert system used for locating solutions to problems in some applications (6).

Previous cyber security methods are outdated in terms of speed. A firewall for cyber security has certain limitations because it is the fortress of the system and is not capable to fight an enemy within the system. The firewall is not capable to fight viruses, Trojan horses, and ransomware within the system. Hence, there is a requirement for intelligent agents and expert support systems (7–8). The lack of skilled

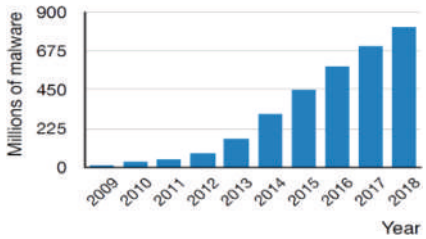

FIGURE 1 | Increment in malware per year (9).

professionals is a major concern for cyber security. More than 75% of cyber security organizations are facing a shortage of skilled professionals, almost 70% of organizations got breached once, and 44% of security alerts remain non-scrutinized. Hence, it is apparent that a considerable amount of attacks remain unnoticed. For an analyst it takes an average of 180 days to detect a breach into the system, during this time, many cyber actors escape unnoticed (9).

Figure 1 shows an increment in malware per year. We have seen a stimulation in cyber attacks by 600% in 2019–2020 due to the global pandemic that was anticipated in a decade. So, the demand for expert alert systems and intelligent agents is obvious.

This paper is organized as follows: the further section includes a literature review and section titled, "Artificial Intelligence and Expert Systems for Cyber Security" illustrates various types of AI and expert systems for cyber security and the section titled, "Conclusion" concludes the review.

Literature review

Machine learning is an important tool in combating cyber threats in a continuously evolving cyber security environment. Explainable artificial intelligence (XAI) methods in cyber security to improve confidentiality are proposed by Mathew (10). The approach is validated with current databases in the domain of cyber security.

To determine the state of cyber security, a model called the machine learning expert system was developed by Patil (11). It is a self-learning expert system for information security. The prototype is based on the modified entropy, which is capable of receiving a fuzzy learning matrix to implement an appropriate decision system for recognizing critical cyber attacks. It is proven that it improves the cyber attack detection effectiveness significantly.

The challenges in the cyber security environment are increasing exponentially nowadays and becoming difficult for human eyes to detect subtle threats and vulnerabilities; hence, a requirement for an expert system is essential. A plan was developed by the United States called Cybersecurity National Action Plan (CNAP) to strengthen cyber security and training. A cloud based intelligent tool called viCyber was presented by Kuppa (12). The system presented is a decision support system that helps analysts make quick and appropriate decisions.

A massive amount of data is being uploaded on the Internet every day with increasing concern for cyber security. The continuous need for updates in security patches is necessary. Hence, the use of deep learning methods can be helpful in a number of situations in cyber security. The various deep learning methods can be used for malware detection, intrusion detection, etc. The deep learning methods for cyber security are presented by Kuzlu et al. (13).

Rapid growth in IoT devices has become a major concern in IoT ecosystem because of increasing vulnerabilities. Reinforcement learning can be used as a security tool to secure the IoT devices. A comprehensive survey on vulnerabilities due to IoT devices is carried out by Maxwell et al. (14). In this paper, the implementation of reinforcement learning algorithms in the cyber security environment and exploitation of challenges is presented. The reinforcement learning algorithms for cyber security include the following:

- Multilayer perceptron algorithm (MLP)
- Convolutional neural network algorithm (CNN)
- Recurrent neural network algorithm (RNN)
- Self-organizing map algorithm (SOM)
- Deep transfer learning algorithm (DTL)

An increment in the number of cyber attacks per year poses a challenge for any organization or federal institution. To counter this problem, a requirement for a cyber security skilled workforce is the topmost priority. CyberMaster is an expert system, which can be used to assist the trainees throughout the training. The development of CyberMaster is performed by Abdullahi et al. (1). It is an expert tool that uses visual instructions to guide the learner throughout the process. This tool is proven to be effective to train the new cyber security workforce to fulfill the increasing demand for skilled experts in time.

Various AI methods are used for protecting the cyber security environment. The use of AI in the cyber security domain is presented by Carlton and Levy et al. (3). In this paper, the various subsets of AI like a machine and deep learning, decision trees, *k*-nearest neighbor, support vector machines (SVM), and artificial neural network (ANN) are used for cyber security. Furthermore, the paper includes future developments and applications of AI in the cyber security domain.

The use of IoT devices has been augmented exponentially, despite concerns for cyber security growing along with it. The important role of AI in the cyber security of the IoT has been presented by Chernyshov et al. (4). This paper reviews the significant and comprehensive role of AI in the cyber security domain. Attackers still are managing to exploit the system; hence, there is an essential need to strengthen the tools and expert systems in order to prevent the attacks. This paper concludes the future developments in the cyber security domain using AI and its alternatives.

FIGURE 2 | Decision tree example for classification of network traffic (4).

An expert system, which is used for rapid intrusion and attack detection, is developed by Da et al. (2021). The proposed tool is flexible and agile in identifying and alerting the administrators about the intrusion in order to perform the counterattack. It is successfully used in simulation to detect the attacks to facilitate warning. The role of this expert system is not to protect the system but alerts the administrators in order to defend the system.

Artificial intelligence and expert systems for cyber security

The various kinds of AI and expert systems that are used for cyber security are discussed below:

Machine learning

There are three kinds of machine learning methods: supervised learning, unsupervised learning, and reinforced learning. Supervised learning is when the training dataset is labeled manually as legitimate or malicious and then it is classified for analysis (4). Unsupervised learning refers to the use of learning and training dataset which is not labeled and classified manually. Reinforced learning is a method in which desired behavior is appreciated and malicious behavior is punished. Any kind of antivirus software is an example of machine learning in the cyber security domain.

Decision trees

It is a decision-support system of AI that uses a tree structure in order to make intelligent decisions. Decision trees are not considered highly appreciable for cyber security but are effective to some extent. Decision trees are mostly used for intrusion and malware detection using an algorithm that plays a small game of questions for the identification and detection of malware. An example of the decision tree is shown in **Figure 2**.

k-nearest neighbors (*k*-NN)

The *k*-nearest neighbor technique (*k*-NN) is an intelligent tool of machine learning that uses supervised learning to find data points near the value of *k*. *k*-NN can be used for systems like intrusion detection because it is designed to learn from exclusive data that manifest certain patterns. This technique is implemented in order to detect proxy data ejection attacks. The determination of data points in clusters using *k*-values is shown in **Figure 3**.

Support vector machines

It is a supervised learning tool of machine learning in order to analyze data for regression analysis and classification. In cyber security, this is used to analyze patterns of Internet traffic and discretization them into several component classes like SMTP, FTP, HTTP, and so on. This technique is useful for the simulation of attacks while training. An example of a support vector machine is depicted in **Figure 4**.

Artificial neural network to counter intrusions

Artificial neural network (ANN) is the field of AI, which is proven to be an important tool for cyber security. ANN is a learning tool that likely functions as the human brain. They can learn and assist while solving problems in challenging environments (3). **Figure 5** shows the use of neural networks to counter intrusions within an integrated environment. Network traffic monitoring can easily be done by ANN. **Figure 2** shows intrusion detection in the delivery phase before a potential attack takes place. ANN is capable to learn from previous attacks and activities in order to strengthen security.

In contrast, the advantage of using ANN for cyber security is that its capability to learn. Earlier, malicious activities

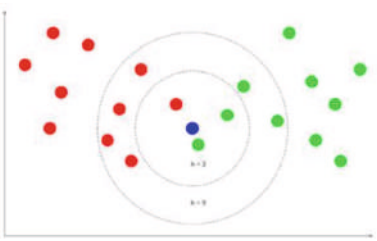

FIGURE 3 | Determination of data points using *k*-values.

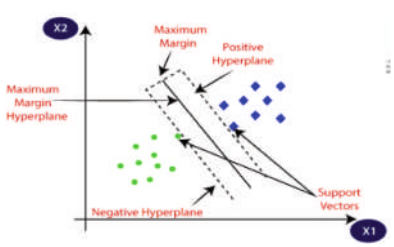

FIGURE 4 | Example of support vector machine (javatpoint.com).

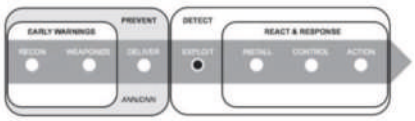

FIGURE 5 | ANN to counter intrusions within an integrated environment (3).

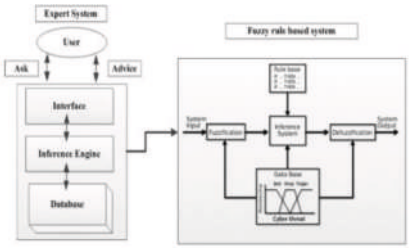

FIGURE 6 | Fuzzy rule based expert system (Da, 2021).

were defined by human experts as per their knowledge. However, now ANN can replace the human force with training for identifying such patterns with precision using previous data.

Deep neural network (DNN) is an expansive form of ANN that has been replacing the traditional ways of defense (15). This tool is used not only to protect federal institutions and organizations from cyber attacks but also to predict potential threats and vulnerabilities.

CyberMaster: An intelligent tool to assist cyber security curriculum development

A computer system that has decision-making ability like humans is called an expert system. These systems are capable to assist humans in quick decisions in various domains. CyberMaster is a system used to guide the development curriculum of cyber security. A user interface, interference engine, knowledge base, and user model are the major components of CyberMaster (1).

Knowledge base

The most essential thing in developing an expert system is to accumulate knowledge. The NICE framework is used to form the knowledge base of CyberMaster. The initial step to building the knowledge base is to identify the total units of knowledge and divide them as per the work roles.

User model

The CyberMaster user model tracks the interaction between the system and the user, which helps in building a model based on user performance. Then this user model sends the accumulated data to the interference engine in order to provide feedback.

Interference engine

The logical rules are applied to the unit of Knowledge Base by interference engine. It also uses the user model and rules from the knowledge base in order to provide tailored feedback to the curriculum designer.

User interface

It gives the privilege to the user to interact with the system. The editing option is also provided, which enables users to modify or create a course.

Fuzzy rule based expert system

This expert system is used for the indication and warning of attacks to the administrators (Da, 2021). The algorithm of the system consists of a bunch of rules to determine the threat and warning is used for facilitating the attack. This tool is not aimed to protect the system under attack but to warn the administrators of the system for quick response. It can be effectively used to determine the nature of the attack performed by the intruder. **Figure 6** shows the structure of a fuzzy rule based expert system.

Intrusion detection and prevention systems

These systems are used for active defense and warning. It effectively prevents the intruder from breaching into the system environment and immediately informs the administrator. These systems tend to monitor the environment continuously to identify suspicious movements and activities within the system environment. It is capable to kick out existing malware, Trojan horse, and other malicious programs and capable to identify social engineering assaults like phishing and man-in-the-middle that exploit users' sensitive information. Prevention systems help prevent attacks like malware injection, malicious applications, and SQL injections.

Conclusion

Artificial intelligence (AI) and expert systems are essential and vital tools to counter potentially dangerous threats in cyber security. The protection of data requires skilled cyber security technicians for various types of roles. The use of AI and expert systems is a need of cyber security in order to defend its environment. AI and its subsets are widely used to protect the cyber security environment. Tools like machine and deep learning, decision trees, *k*-NN, and support vector machines are widely used for cyber security in order to make intelligent decisions. The essential role of an expert system

is to monitor the threats and assist the administrators to strengthen security.

References

1. Abdullahi M, Baashar Y, Alhussian H, Alwadain A, Aziz N, Capretz LF, et al. Detecting cybersecurity attacks in internet of things using artificial intelligence methods?: a systematic literature review. *Electronics.* (2022) 11:198.
2. Bertino E. AI for security and security for AI. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*. New York, NY: ACM Press (2021). p. 333–4. doi: 10.1145/3422337.3450357
3. Carlton M, Levy Y. Expert assessment of the top platform independent cybersecurity skills of non-IT professionals. *Proceedings of the SoutheastCon 2015*, Fort Lauderdale, FL. (2015). doi: 10.1109/SECON.2015.7132932
4. Chernyshov VA. Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems. *J Theoret Appl Inform Technol.* (2017) 95:1705–14.
5. Donepudi PK. Crossing point of artificial intelligence in cybersecurity. *Am J Trade Policy*. (2015) 2:121–7.
6. Goode J. Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online J Appl Knowl Manag.* (2018) 6: 67–80.
7. Göztepe K. Designing a fuzzy rule based expert system for cyber security. *Int J Inform Secur Sci.* (2012) 1:13–9.
8. Hodhod R, Khan S, Wang S. CyberMaster?: an expert system to guide the development of cybersecurity curricula. *Int J Online Biomed Eng.* (2019) 15:70–81.
9. Hodhod R, Wang S, Khan S. Cybersecurity curriculum development using AI and decision support expert system. *Int J Comput Theory Eng.* (2018) 10:111–5. doi: 10.7763/IJCTE.2018.V10.1209
10. Mathew A. Deep reinforcement learning for cybersecurity applications. *Int J Comput Sci Mobile Comput.* (2021) 10:32–28. doi: 10.47760/ijcsmc.2021.v10i12.005
11. Patil P. Artificial intelligence in cyber security. *Int J Res Comput Applic Robot.* (2016) 4:1–5.
12. Kuppa A. Adversarial XAI methods in cybersecurity. *IEEE Trans Inform Forensics Secur.* (2021) 16:4924–38. doi: 10.1109/TIFS.2021.3117075
13. Kuzlu M, Fair C, Guler O. Discover internet of things role of artificial intelligence in the internet of things (IoT) cybersecurity. *Discover Internet Things.* (2021) 1:7. doi: 10.1007/s43926-020-00001-4
14. Maxwell P, Alhajjar E, Bastian ND, Maxwell P, Bastian ND. Intelligent feature engineering for cybersecurity. *Proceedings of the 2019 IEEE International Conference on Big Data (Big Data)*, Los Angeles, CA (2019). p. 5005–11. doi: 10.1109/BigData47090.2019.9006122
15. Naik B, Mehta A, Yagnik H, Shah M. The impacts of artificial intelligence techniques in augmentation of cybersecurity?: a comprehensive review. *Complex Intellig Syst.* (2021) 8:1763–80.