EasyChair Preprint

№ 3955

Using Artificial Intelligence for Intrusion Detection System

Satish Khadka

July 27, 2020

Using Artificial Intelligence for Intrusion Detection System

Satish Khadka
Fundamentals of Computational Intelligence
Flinders University

Khad0063@flinders.edu.au

Abstract

Today in the field of Information and Technology everything is trying to be automated for reliability and better results. Nowadays information is a critical aspect among every organization. There are billions of users connected to the internet these days, all of them have some significant confidential information. The most important asset these days are the information related to the organization or users of that organization. Various kinds of hackers are trying to break into an organization's system to gain access and retrieve all sensitive information that could compromise the network resulting in great risk to the organization. To make a system secure, Intrusion Detection System (IDS) is the key component, which will notify the organization if someone is trying to break into their system and also provides a possible way to deal with it. Various IDS approaches are being used however; they are relatively ineffective. To make the information system more secure Artificial Intelligence can play a vital role. Artificial Intelligence will provide better results in intrusion detection by using neural networks and fuzzy logic with network profiling. This literature review will try to point out the difference between the IDS without using AI and using IDS with AI and the benefits of using AI in the field of IDS.

1 Introduction

The most important thing for any organization these days is information. Information is stored by organizations these days to process it on the network-based system for specific purposes. It is necessary for the system in the organization to be protected because of the global use of e-commerce. Confidentiality, integrity, and availability (Idris, N., & Shanmugam, B. (2005) are the key factor for any organization while developing any IT or Software product. The various kinds of attacks can be detected and prevented by the intrusion detection system. It can also react to the attacks that can occur in a network-based system. In information security, the intrusion detection system is a very important factor however, building a system without vulnerabilities is not possible.

2 Current Intrusion Detection System

Intrusion Detection can be defined as a process which identifies an occurring or ongoing attack on a network-based system and analyze if there is any violation of security policy.
Idris and Shanmugam 2005, argue that the main purpose of the intrusion detection system is to protect the availability, confidentiality and integrity of information of the organization. IDS can be divided into two classes: Host-based or Network-based system which can be used to determine either anomaly detection or misuse detection. Misuse detection depends on verifying previously known patterns of attacks against the database and it is effective for determining the known attacks however it can't determine new security attacks. Anomaly detection deals with something unusual by applying statistical measures or artificial intelligence to differentiate current activity against historical knowledge. It requires huge training data for artificial learning algorithm. There are some IDS which is a combination of both the Host-based and Anomaly-based system which is also referred to as the Hybrid system. For both misuse detection and anomaly detection techniques, Artificial Intelligence technique has been applied (Idris, N., & Shanmugam, B. (2005).

3 Problems in Intrusion Detection

Data collection, data reduction, behavior classification, reporting and response are the issues related to Intrusion Detection (Highland, H. (1995)). Data reduction can be referred to as analyzing the collection of data which will figure out the key component of the data and results in reducing the processing time, communication overhead and storage requirements. There is a massive amount of data audit available because of which it is difficult to classify the data by hand. Due to this reason it is important to deduct data by filtering the data that is regarded as not useful data. To find out the hidden patterns of data, data can be grouped or clustered and to minimize the overhead, characteristics of clusters can be stored instead of data. Behavior classification can be defined as the process of identifying attackers and intruders. It is very difficult to classify user or system behavior. There is only a fraction of difference between normal users and intruders as a result of which the classification results in 'false negative' and an attacker is misclassified as a normal user.

4 Artificial Intelligence Technique in Intrusion Detection

The use of Artificial Intelligence is to design and develop an Intelligent Intrusion Detection System (IIDS) which will accurately determine 'false alarm' or very less 'false alarm' and can't be easily cheated by little variation in patterns and achieved in real-time. Intelligent Intrusion Detection System is not just an Intrusion Detection System, it is capable of discovering attack patterns, determining new attacks based on previously known attacks. The ultimate goal of using AI in IDS is to build a system that is capable of differentiating various kinds of attacks in a networked-based system.

4.1 Neural Network Approach

Neural Network approach is one of the popular AI technique which is applied in IDS and in the past, there were huge amount of research conducted to apply it on IDS. Neural networks were typically developed to learn the typical characteristics of the system's user and determine statically important difference from the beginning.

4.2 Decision tree-based technique

For classification and prediction, decision trees are the most powerful and popular tool. Nodes, arcs and leaves are the three components of a decision tree. Among other, node is the most informative attribute, each arc is labeled with feature value and each leaf is labeled with a category or class ((Kumar, Gulshan, Kumar, Krishan, & Sachdeva, Monika. (2010))).

4.3 Fuzzy logic technique

Intrusion detection can be benefited by using fuzzy logic in two different ways, firstly, various parameters are used in intrusion detection such as CPU usage time, connection time, etc. are considered as fuzzy variables. Secondly, the security concept is fuzzy itself. Using fuzzy logic in IDS is to make it easier to determine the separation between the normal and abnormal behavior of the user. Fuzzy logic and data mining technique was applied by Dickerson, J.E, & Dickerson, J.A. (2000), to detect intrusion in network. They have proposed FIRE (Fuzzy Intrusion Recognition Engine) which uses the fuzzy logic to determine if there is any malicious activity in the network-based system (Dickerson, J.E, & Dickerson, J.A. (2000)).

4.4 Genetic algorithm-based technique

A genetic algorithm is a searching technique that can be used to find appropriate to optimization and search problems (Kumar, Gulshan, Kumar, Krishan, & Sachdeva, Monika. (2010)). To separate normal network traffic and abnormal traffic, a genetic algorithm is massively used in the field of intrusion detection. To learn different user behavior and identify abnormal user activities, Balajinath, B., & Raghavan, S. (2001) used a genetic algorithm where user behavior can be determined by the 3-tuple <Match index, Entropy index, Newness index>.

5 Artificial Intelligence and Intrusion Detection

AI can be defined as a science whose objective is to find the importance of intelligence and built

intelligent machine, or it can be defined as a science which finds a solution for various complex problems without which such complex problems cannot be solved. An intelligent agent system comes under an AI approach called as Computational Intelligence (CI), which consists of various nature-inspired techniques such as neural networks, fuzzy logic, evolutionary computation, swarm intelligence, machine learning and artificial immune systems (AIS) (Dilek, S., Çakır, H., & Aydın, M. (2015)). AISs are capable of continuous and dynamic learning because it is a part of the computational model and designed to mimic natural immune systems in application for computer security in general and intrusion detection in particular. Another example of the AI approach is a genetic algorithm that is based on machine learning which shows the process of natural section and can provide robust, adaptive and optimal solutions for various complex problems. Specific rules for various security attacks in IDSs can be made and it can be used to classify the various kinds of cyber-attacks. Even though there are various methods deployed over networks and the internet for securing data, an intruder always finds a new approach to attack network-based systems. A software or hardware which is placed in the network and can detect possible intrusions and also attempts to prevent them is called as intrusion detection and prevention system (IDPS). Monitoring, detecting, analyzing and responding to unauthorized activities are the four crucial security functions an IDPS must impose (Dilek, S., Çakır, H., & Aydın, M. (2015)).

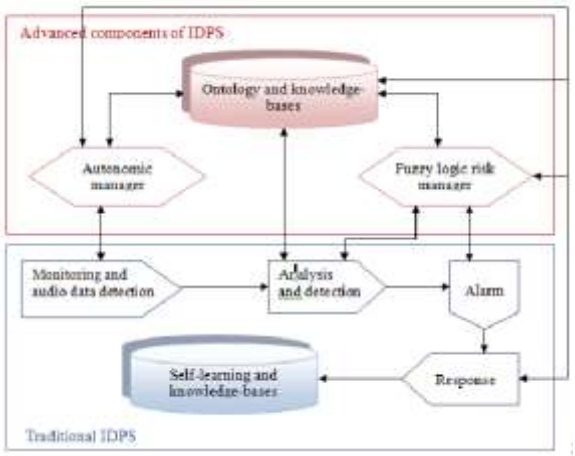

Fig: A typical IDPS (Patel, A., Taghavi, M., Bakhtiyari, K., & Celestino Júnior, J. (2013))

6 What are the challenges of Cyber Security?

These days cybercriminals are trying to use different kinds of methods to attack a target to (i) steal personal data which poses sensitive information such as, financial information; or (ii) gaining access to target's machine to perform malicious activities like, infecting with malware, encrypting data (Conti, M., Dehghantanha, A., & Dargahi, T. (2018)).

It is believed that most of the time an intruder leaves tracks when trying to exploit the target. To gather cyber intelligence, the integrated security approach (ISA) requires collecting and analysis of various range of information. There are challenges in gaining relevant data tracks, they are: (i) Amount of data: As there is an exponential growth of usages of electronic devices information from the whole organization may need to be considered while trying to implement an ISA., (ii) Heterogeneity of data and their sources: Due to the difference between data and it's origin, it is hard to discover and gather those data. Even if the relevant heterogeneity within the cyber environment is discovered, systems and networks topology and behavior may change and because of which it requires constant adaption., and (iii) High data velocity: The challenges arise in storing data and processing it because of the rate at which produced and processed within its sources (Wirkuttis, N., & Klein, H. (2017)).

7 Benefits of AI in Cyber Security

Those organizations which have adopted AI in cybersecurity are experiencing high benefits and two out of three firms are saying that AI has increased the return of investment on cybersecurity tools.

7.1 Minimization of cost to detect and respond to breaches

When an organization uses AI for cybersecurity, it allows them to figure out and reuse previously known threat patterns to identify and discover new threats. As a result of which there is a significant reduction in time and effort that are used to identify, investigate and remediate threats. About 64% of the executives said that the usage of AI in the field of cybersecurity has decreased the cost to detect and respond to

breaches. Most of the organizations experienced 1-15% of cost reduction while using AI for defending against cyber-attacks.

7.2 Quick response to breaches

To minimize the cost of breaches, an organization needs to respond as soon as possible otherwise different kinds of attacks can impose a greater threat to information and assets of the organization. So, a quick response is a key to make an organization secure. The average time taken for identifying attacks and breaches is decreased by up to 12% for organizations when AI is used. Moreover, for an attack, the time taken to remediate a breach or implement patches reduced by 12% (LAZIĆ, L. (2019)).

8 Drawbacks of AI in Cyber Security

Apart from its benefits, there are some drawbacks of AI while implementing in the field of cybersecurity such as (i) Inability to maintain cyber security autonomously: Even though there are advantages of using AI in cybersecurity, lack of completely autonomous in security system requires human inter-reaction as a result of which it can't replace human decision completely., (ii) Data privacy: As AI uses techniques like Artificial Neural Networks and Deep Neural Networks, private and public organization are worried about their personal data as it requires huge amount of data analysis., (iii) Ethical concerns: The decision made by AI-based security system does not have moral code so, the decision made could differ from the one that a person would make (Wirkuttis, N., & Klein, H. (2017)).

9 Future of Artificial Intelligence and Intrusion Detection System

As information related to individuals or organizations are very important, we need better cybersecurity defense techniques which ensure the confidentiality, availability, and integrity. It is evident that there are limitations of human and the fact that agents like computer viruses and worms are intelligent so, there is a necessity of intelligent cyber agent which will be able to detect, evaluate and respond to cyber-attacks as quick as possible. Planning and future research will be required for the application of AI techniques in cyber defense. With the help of automated knowledge management, it can be guaranteed that rapid assessment of the situation and superiority of decision can be achieved. It can be foreseeable that soon we will achieve technological creation that is smarter than human intelligence. To develop a trustworthy, deployable intelligent agent system that has capabilities to manage distributed resources we require more research in the field of cybersecurity and artificial intelligence.

IDPSs should be enhanced in such a way that we can create hybrid IDPS which will improve the performance of anomaly intrusion detection by combining unsupervised learning algorithms and new techniques (Dilek, S., Çakır, H., & Aydın, M. (2015)).

Overall, AI technique should be able to understand how non-intrusive and intrusive behavior differs and it should also be able to enable hierarchical classification of different types of attacks (Highland, H. (1995)).

10 Conclusion

Nowadays, every company and organization is connected to the internet and the data related to them has significant importance that might be either individuals or organizations. To store and process, such data extra security mechanisms must be used so that attackers will not be able to break in and steal information or gain access to the target and perform malicious activities. To ensure the safety and privacy of the user's data organization are using various cybersecurity approaches and even hiring security specialists. However, attackers or intruders manage to find their way to break into the system because viruses and worms seem to become more intelligent than human beings. To prevent cyber-attacks an intelligent approach is required and it can be achieved by using AI in the field of cybersecurity so that whenever someone tries to break into a system, the intelligent agent must able to detect and prevent the system from unauthorized actions.

References

Balajinath, B., & Raghavan, S. (2001). Intrusion detection through learning behavior model. Computer Communications, 24(12), 1202-1212.

Conti, M., Dehghantanha, A., & Dargahi, T. (2018). Cyber Threat Intelligence : Challenges and Opportunities.

Dickerson, J.E, & Dickerson, J.A. (2000). Fuzzy network profiling for intrusion detection. PeachFuzz 2000. 19th International Conference of the North American Fuzzy Information Processing Society - NAFIPS (Cat. No.00TH8500), 301-306.

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. 6(1), 21-39.

Highland, H. (1995). Artificial Intelligence and Intrusion Detection: Current and Future Directions : Jeremy Frank, University of California, Davis, CA. Computers & Security, 14(1), 31.

Idris, N., & Shanmugam, B. (2005). Artificial Intelligence Techniques Applied to Intrusion Detection. 2005 Annual IEEE India Conference - Indicon, 2005, 52-55.Association for Computing Machinery. 1983. *Computing Reviews*, 24(11):503-512.

Kumar, Gulshan, Kumar, Krishan, & Sachdeva, Monika. (2010). The use of artificial intelligence based techniques for intrusion detection: A review. Artificial Intelligence Review, 34(4), 369-387.

LAZIĆ, L. (2019). BENEFIT FROM AI IN CYBERSECURITY. *The 11th International Conference on Business Information Security (BISEC-2019), 18th October 2019, Belgrade, Serbia*

Novikov, D., Yampolskiy, R., & Reznik, L. (2006). ARTIFICIAL INTELLIGENCE APPROACHES FOR INTRUSION DETECTION. 2006 IEEE Long Island Systems, Applications and Technology Conference, 1-8.

Patel, A., Taghavi, M., Bakhtiyari, K., & Celestino Júnior, J. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications, 36(1), 25-41.

Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *'Cyber Intelligence, and Security Journal*, *1*(1), 21-23.