International Journal of Cyber-Security and Digital Forensics (IJCSDF) 9(1): 34-41
The Society of Digital Information and Wireless Communications (SDIWC), 2020 ISSN: 2305-0011

A Survey of Artificial Intelligence Techniques for Cybersecurity Improvement

Athari M. Alrajhi
Computer Science Lecturer, Department of Libraries and Information, College of Arts, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
amalrajhi@iau.edu.sa

ABSTRACT

In the last years, cybersecurity has become the most important issue. Many researchers have investigated the development of cybersecurity tools, and several solutions have proposed to protect computer systems from attacks. However, the old traditional ways can no longer be relied upon. This paper introduces the need for the development of cybersecurity skills in an innovative way and how artificial intelligence can be implied to improve many security systems such as intrusion detection systems. A lot of companies around the world adopt AI techniques to enhance their systems safety and to optimize nearly everything. Then, it comes to no surprise that AI is radically transforming cybersecurity.
In this paper, the advanced cybersecurity solutions driven by artificial intelligence for improving intrusion detection systems are discussed, as well as an explanation of the advantages and the disadvantages of existing methods. Furthermore, some promising future research directions are introduced.

KEYWORDS

Artificial Intelligence, Cybersecurity, Security, Intrusion Detection, Attacks, Threats, AI.

1 INTRODUCTION

Artificial intelligence (sometimes called machine intelligence) can be defined as the ability of computers to perform tasks that are associated with intelligent beings. AI has shown tremendous growth in the last 20 years. AI can be categorized into 1) weak AI 2) strong AI. Strong AI is where the machine could have common sense, self-awareness, and creativity (human-like intelligence). Weak AI is performing intelligent human processes without really understanding the process that is being done. Also, weak AI completes a task where strong AI completes multiple intelligent tasks. Existing systems are all weak AI systems, where strong AI still does not exist.

AI has many techniques such as machine learning, deep learning, speech recognition, natural languages processing etc. AI can be used in many areas including but not limited to healthcare, gaming, problem solving, finance, education, self-driving cars, cybersecurity and many more as shown in figure 1.

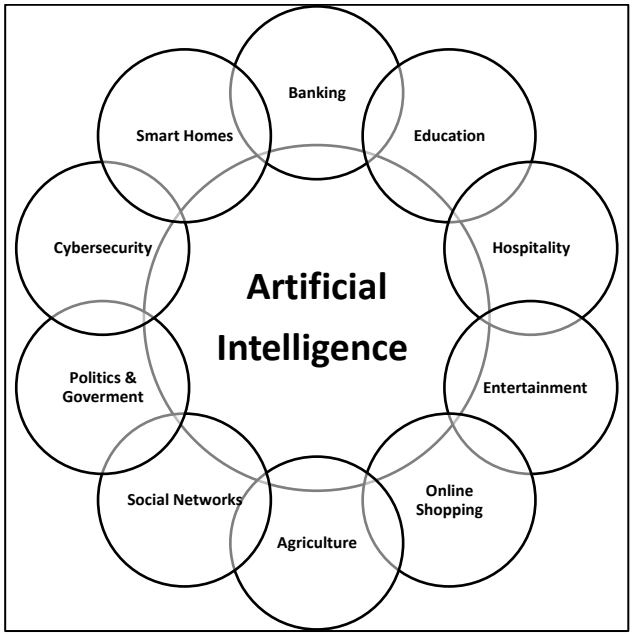

Figure 1. Usages of Artificial Intelligence

Adding artificial intelligence techniques to security systems can reduce the threats of

cybersecurity tremendously. As data acquisition is getting hugger in size, to a point it is difficult for humans to handle, as well as storage capabilities and computing power increasing there is a need for a comfortable and efficient way to handle all of this. So, organizations and experts are using AI with machine learning to reduce the data processing in milliseconds which will lead the organizations to quickly identify threats and recover from them.

Artificial intelligence techniques can be also utilized to improve the access control and the authentication procedures used in different systems. As the saying each coin has two sides so does artificial intelligence. AI can be used to do good as mentioned previously and it can be used to steal private information and perform huge dangerous attacks. This risky side of AI arises due to the possibility of manipulating AI methods so that it can perform in a preferable way to the attackers [1].

In this paper, we'll cover how AI improves cybersecurity in terms of intrusion detection, as well as, provide some future directions for AI and cybersecurity.

2 APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Extent of threats in computer systems and networks has grown beyond the point where people can control them. Since the amount of data to be used in security threats detection and prevention cannot be handled by humans [1]. Therefore, it became necessary to automate threats management. Furthermore, as threats are dynamically evolving, developing software with classic fixed techniques for effectively defending against such attacks became difficult. In fact, security attacks often change their appearance which considered one of the main challenges for cybersecurity. As a result, when a new kind of attack strikes, even common security solutions often fail to detect and prevent these intelligence threats, as there are no previous patterns against which it can be matched. Thus, it is evident that the detection and prevention of intelligent attacks can be achieved only by an intelligent tool [1],[2]. So, this issue can be handled by applying techniques of artificial intelligence that play an essential role in cybersecurity. AI can be a powerful tool in detecting and fighting the latest security threats. Therefore, employing AI in cybersecurity can improve its performance and help in building a solid defense against new attacks.

AI offers numerous methods for cybercrime detection and prevention such as neural networks, deep learning, intelligent agents and immune systems, pattern recognition, machine learning, fuzzy logic, etc. [3],[4]. These mechanisms depend on simulating human behavior to take an appropriate decision. They are able to analyze huge amounts of data and learn continuously from those data to adapt to changes and new security threats. This type of learning makes it possible to design automated detection systems. AI algorithms could help not only providing threats detection, but also take proactive actions to remediate certain situations. Moreover, they can defend against security attacks and categorize malware and threats, eventually protecting computer systems.

3 AI-BASED INTRUSION DETECTION AND CLASSIFICATION TECHNIQUES

Although computer networks within organizations provide communication and facilitate business transactions, this interconnectivity among computers can be exploited by malicious users to misuse resources and launch security attacks. Intrusions are one of such attacks that pose a severe risk in computer systems and networks environment. Several intrusions can compromise the security objectives namely, availability, integrity and confidentiality. To stop such attacks, a number of intrusion detection systems (IDS) have been designed [5].

IDS is an effective technique to detect, prevent and react to the computer attacks [6]. The main goal of IDS is to detect the anomaly and suspicious behavior of the host or network and report it and consequently enable administrators to avoid it in the future [7]. However, the continuously growing attacks pose critical challenges to develop an adaptive and flexible IDSs. Therefore, in order to detect new intrusions, researchers have employed artificial intelligence techniques in the intrusion detection system to improve its work. AI techniques play a notable role in the development of IDS. AI-based IDS is capable of learning and recognizing new attacks by analyzing a large amount of data.

In fact, there are three types of intrusion detection techniques namely, statistical, knowledge-based and artificial intelligence-based techniques, as illustrated in figure 2. Statistical techniques use a statistical model for defining the observed behavior of the system. While knowledge-based IDS techniques use expert system to capture the observed behavior [7], [8]. On the other hand, AI-based IDS techniques used to determine a suitable classification model to recognize normal and abnormal behavior. In this paper, we will focus on the third type which based on using some approaches such as genetic algorithm, neural network, fuzzy logic, artificial immune system, etc. for intrusion detection. An overview of the applications of these AI techniques to intrusion detection is discussed in the following subsections.

3.1. Neural Network (NN)

Neural Network (NN) mimics the human brain to create an information processing system which consists of large number of interconnected nodes (neurons) working with each other to solve a specific task. The output of each node is weighted and processed to fed as an input to all other nodes in the next hidden layer. The self-learning process that generated by the architecture of neural networks makes it capable of capturing highly complex and non-linear relationships between data [9]. Figure 3 shows the architecture of NNs.

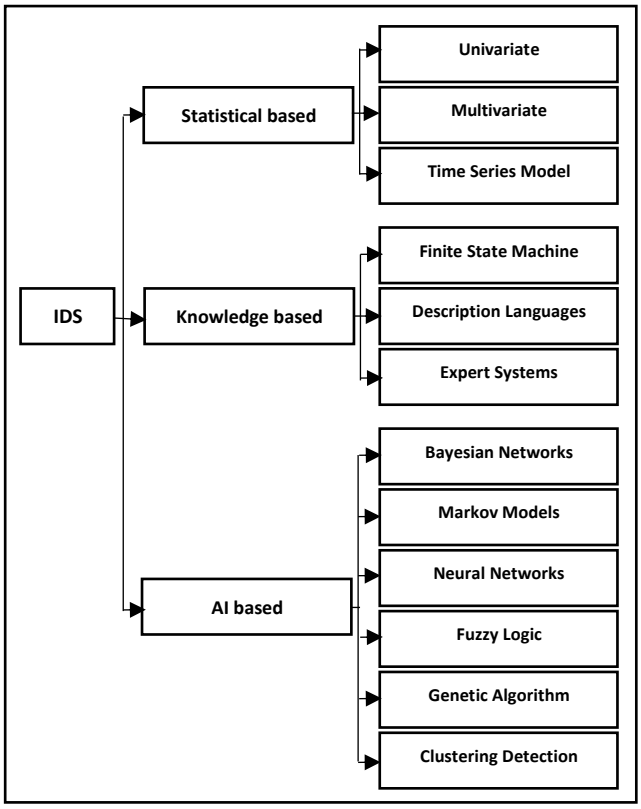

Figure 2. Intrusion Detection Techniques

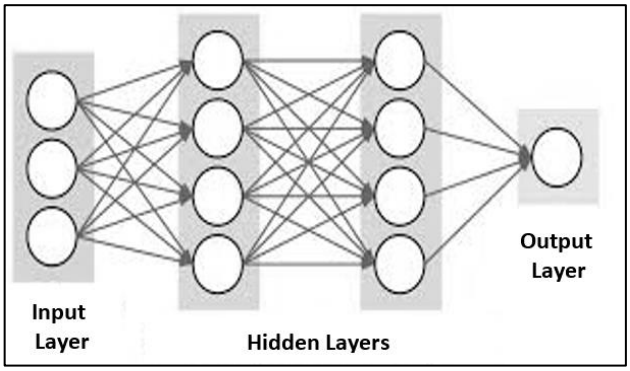

Figure 3. Architecture of Neural Networks

NNs can extract the patterns, detect the relationships in data and learn through experience in order to gather knowledge. The idea behind the application of NNs in IDSs is to include an intelligent agent in the system that is able to disclose and analyze the normal and abnormal behavior of system users. If properly designed, NN can address many problems of other approaches. The main advantage of NN is its ability to infer solutions from collected data

without having any prior knowledge of the regularities in these data. This in combination with their ability of generalization from learned data which enables NN to detect and classify unknown attacks and different types of the known attacks. Further, once an attack recognized by NN, it cannot take place in the future. The speed is also another advantage of the neural network. All these properties have made NN an appropriate method for intrusion detection. In order to apply this method to IDS, data representing attacks and non-attacks should be introduced to the NN to adjust network coefficients automatically during the training phase [6], [7], [8], [10].

In the last few years, many researches have investigated the application of NNs to intrusion detection [11]. One of the most recent studies has been prepared by Yaser A. Jasim [12]. In this work, the Backpropagation Neural Network is used due to its ability and speed to recognize packet patterns obtained from the network to detect intrusion of the system. Many attacks features have been extracted and analyzed of both standard and unusual packets. The analyzing results of these packets have been used to learn the NN on the pattern of both types of packets using standard Backpropagation algorithm. The experimental results show that the system can recognize the standard packets from the unusual ones and also classify them into different five types with efficiency reaches 100%.

Another approach is proposed by A.Alhello and Kaur [13] to generate artificial neural networks (ANNs)-based model which is able to detect intrusions in a system and to give alerts. In this work, data of 100 datasets have been trained to learn ANNs. The results prove that this model is a robust model for intrusion detection.

In order to overcome the low detection rate, high rate of false positives and other defects of IDS, a new intrusion detection algorithm based on a fuzzy neural network is presented by Liang [14]. This algorithm classifies objects and recognizes normal and abnormal behaviors. It is demonstrated through extensive experiments that the proposed model is feasible, effective and has a better generalization. In addition, the rate of correct intrusion detection is increased, and the false detection rate is reduced.

3.2. Fuzzy Logic (FL)

Fuzzy logic deals with reasoning that is approximate rather than exact and fixed. Its variables values may range between 0 and 1, and its truth value may range between completely false and completely true. Fuzzy logic builds on a set of human language rules provided by the user. Then, these rules are converted to their mathematical equivalents in order to make strict decisions. Due to its simplicity and flexibility, fuzzy logic techniques have been employed in the area of computer security, especially in intrusion detection. The fuzziness concept helps to smooth out the abrupt separation of usual behavior from unusual behavior. Fuzzy logic can handle problems with incomplete and imprecise data. Therefore, it is able to represent those imprecise forms of reasoning in some areas where firm decisions should be made in undefined environments like intrusion detection [6], [15], [16].

Recently, several researchers around the world focused on fuzzy rule learning for efficient intrusion detection using data mining techniques. Yu and Wu [17] proposed a novel model based on naïve Bayes classification (a data mining technique) to classify system call sequences of privileged processes as “anomalous” or “normal” to detect anomaly intrusions. The frequency of each system call is provided as the basis of the classifier. The probabilities ratio of a sequence generated from a process and not from the process is provided as the input to a fuzzy system for the purpose of classification. The results show that the suggested model can effectively detect most of the intrusion traces with a low rate of false alarms.

Another fuzzy model based on data mining techniques has been proposed by Chapke and Deshmukh [18]. This model is developed with the aim of improving the intrusion detection rate of the existing IDS using C4.5 data mining technique, which is a modified version of the Apriori algorithm. Moreover, it aims to generate alerts and detect all types of malicious users. The analysis of performance results in higher detection rate and lower false positive rate when compared with other systems.

A combination of some AI techniques is another manner which followed by many researchers to improve the performance of IDS. For example, Dixit and Ukarande [19] presented improved IDS based on fuzzy logic and neural network. The fuzzy system used a defined set of rules to classify the test data as normal or anomalous and detect the intrusion behavior in the network. Whereas neural network trains and tests the data for intrusion detection. The evaluation depicts the effectiveness of the proposed model in terms of obtaining good precision in attack detection.

3.3. Genetic Algorithm (GA)

The genetic algorithm is an optimization technique to find approximate solutions to search problems. It begins with a set of random or selected solutions called chromosomes. The entire set of these chromosomes forms a population. The algorithm works iteratively which enables the chromosomes to improve during these iterations or generations. Eventually, the best solution is generated [20], [21]. The GA has been extensively employed in the domain of intrusion detection to recognize normal network traffic from anomalous one. Each time there is a new attack, the GA-based IDS will update itself automatically to detect new malicious activities. This makes the GA for better than any technique presents in the intrusion detection field [7].

Many researchers have used GA for intrusion detection in different ways [22]. Some researchers have used it directly to derive classification rules, while others use it to select convenient features, while different techniques of data mining are then used to obtain the rules [6]. Gupta and et al. [23] developed a robust intrusion detection using GA to detect the network intrusions. This study aims to develop IDS which adapt itself with changing time. The initial population of GA includes the previously detected attacks. The selected chromosomes consist of those attack patterns which have a high probability to change in the new patterns. Therefore, this enables the system to detect new attack pattern. The results show that the system is very helpful in detecting different types of attacks on the network.

Another approach is suggested by Pawar and Bichkar [24]. They used GA with variable length chromosomes for intrusion detection. In this work, fewer chromosomes are used for rule generation, since each one is a complete solution to the problem. Each of these chromosomes will have a limited number of rules. After the classification rules have been generated, the fittest rule is taken for the purpose of detection. Then, this rule is used to classify normal and abnormal behavior. Using fewer chromosomes reduces the search space. Further, the experiments prove that the suggested approach is effective in network intrusion detection. A combination of GA and fuzzy logic technique is presented by Jongsuebsuk et al. [25] for intrusion detection. The aim of this work is to detect new or unknown network attack types. The fuzzy system generates fuzzy rules which later are used by GA to make them able to learn new types of attacks by themselves. After the training phase, the system with the obtained rule can detect network attacks. The results show that the Fuzzy GA is able to detect new and unknown attack types with low false positive rate and high accuracy.

3.4. Artificial Immune System (AIS)

AIS is inspired by the biological immune system which transform the biological models and functions of the immune system into

mathematical models in order to help solve problems [26]. Basically, AIS is based on a number of algorithms. The negative selection is one of the most significant of these algorithms that fits naturally into the field of intrusion detection due to its ability to differentiate between self and non-self. In the case of anomaly detection, the algorithm provides a set of exemplar pattern detectors trained on normal patterns that detect anomalous or unseen patterns.

To construct the detection set, Shen and Wang [27] used the negative selection algorithm to generate random immature detectors. Then, these immature detectors are compared with the normal network parameter patterns. If there is a matching between a random pattern and a normal pattern, the immature detector will be rejected and deleted. Those which do not match any normal patterns will be kept as mature detectors. In the detection stage, a monitored network parameter pattern is compared with mature detectors in the detection set. If it is matched with any mature detector, then an intrusion is detected. The experiments prove that the system has an excellent detection accuracy.

To achieve higher accuracy in intrusion detection, a new detector generation algorithm for AIS-based intrusion detection is proposed by Tabatabaefar et al. [28]. In this work, negative and positive selection algorithms are used to generate antibodies for both types normal and attack records in order to save normal samples. Immature detectors are generated and then trained for each type separately. Simulation results show that the presented algorithm improves the detection rate and reduces the detection time.

Although AI techniques achieved excellent results in terms of improving the intrusion detection systems, they have some limitations that can affect the intrusion detection performance [29]. Table 1 summarizes some advantages and disadvantages of the mentioned AI techniques in the intrusion detection domain.

Table 1. Advantages and Disadvantages of AI-based Intrusion Detection Techniques

Technique	Advantages	Disadvantages
NN-based IDS	• Classifies unstructured network packets effectively. • Multi-layers in NN increase efficiency of classification.	• Requires long time at training phase. • Requires large number of samples for training effectively. • Less flexible than others.
FL-based IDS	• Has better flexibility to some uncertain problems.	• Detection accuracy is lower than NN.
GA-based IDS	• Used to select best features for detection. • Has better efficiency.	• It is a complex method to represent a problem. • Used in specific manner rather than general.
AIS-based IDS	• Provides excellent detection accuracy.	• Requires large number of parameters.

4 Future Directions

Using AI in cybersecurity is often mentioned in papers. However, most of these papers used pre-existing AI techniques and applied them to different aspects of security such as intrusion detection. This may work in a few cases due to some limitations of AI techniques as we mentioned before. Therefore, new AI tools will have to be developed in the future to fit the specific needs of security.

Many new AI tools could be inspired from existing ones to be suitable for security. This makes AI useful to solve other security issues. Thus, not only AI can improve security but also security can be an area of development of AI.

5 CONCLUSION

Security threats have become so varied and smart, that traditional techniques don't seem to be a viable approach anymore. So, it became

necessary to automate threats management using AI techniques. Therefore, we intended to provide the most important effective solutions by discussing many AI techniques that have proven their effectiveness and success in detecting security attacks and threats, and these methods have been compared to clarify the advantages and disadvantages for each one.

There are multiple levels of connections between AI and cybersecurity. In this paper, we have introduced some levels of these connections between both fields in order to improving intrusion detection systems. The demand for utilizing these connections to enhance the performance of the cybersecurity and intelligent aspect of applications from different domains should encourage experts from these two fields to cooperate their efforts in this intersection.

Ultimately, we must be aware that though artificial intelligence plays an essential role to improve security performance, it is a double-edged sword. Artificial intelligence can become a risk to security since it can be exploited by attackers to launch attacks.

REFERENCES

[1] E. Tyugu, "Artificial Intelligence in Cyber Defense," in *3rd International Conference on Cyber Conflict*, 2011, pp. 95–105.

[2] A. N. Jaber, M. F. Zolkipli, H. A. Shakir, and R. Mohammed, "Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing," in *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2017, pp. 241–252.

[3] Z. Siddiqui, M. S. Husain, and S. Yadav, "APPLICATION OF ARTIFICIAL INTELLIGENCE IN FIGHTING AGAINST CYBER CRIMES: A REVIEW," vol. 9, no. 2, pp. 118–122, 2018.

[4] A. Jaber and S. Rehman, "FCM – SVM based intrusion detection system for cloud computing environment," *Cluster Computing*, vol. 6, pp. 1–11, 2020.

[5] S. Anwar, A. Karim, J. Zain, and Z. Inayat, "A Static Approach towards Mobile Botnet Detection," in *2016 3rd International Conference on Electronic Design (ICED)*, 2016, pp. 563–567.

[6] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: A review," *Artificial Intelligence Review*, vol. 34, no. 4, pp. 369–387, 2010.

[7] A. Gupta, B. Singh Bhati, and V. Jain, "Artificial Intrusion Detection Techniques: A Survey," *International Journal of Computer Network and Information Security*, vol. 6, no. 9, pp. 51–57, 2014.

[8] A. Jahan, "Intrusion Detection Systems based on Artificial Intelligence," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 705–708, 2017.

[9] B. Subba, S. Biswas, and S. Karmakar, "A Neural Network Based System for Intrusion Detection and Attack Classification," in *2016 Twenty Second National Conference on Communication (NCC)*, 2016.

[10] A. P. S, G. P. U, and S. K. K, "ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 3, pp. 122–124, 2018.

[11] A. N. Jaber, M. F. Zolkipli, M. A. Majid, and S. Anwar, "Methods for Preventing Distributed Denial of Service Attacks in Cloud Computing," *Advanced Science Letters*, vol. 23, no. 6, pp. 5282–5285, 2017.

[12] Y. A. Jasim, "Improving Intrusion Detection Systems Using Artificial Neural Networks," *Advances in Distributed Computing and Articial Intelligence Journal*, vol. 7, no. 1, pp. 49–65, 2018.

[13] A. A. Z. A.Alhello and H. Kaur, "APPLICABILITY OF NEURAL NETWORK IN INTRUSION DETECTION AND PREVENTION," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, pp. 494–499, 2017.

[14] H. Liang, "An improved intrusion detection based on neural network and fuzzy algorithm," *Journal of Networks*, vol. 9, no. 5, pp. 1274–1280, 2014.

[15] P. Sarathi Bhattacharjee and S. Ara Begum, "Fuzzy Approach for Intrusion Detection System: A Survey," *International Journal of Advanced Research in Computer Science*, vol. 4, no. 2, pp. 101–108, 2013.

[16] N. B. Idris and B. Shanmugam, "Artificial intelligence techniques applied to intrusion detection," in *Proceedings of INDICON 2005: An International Conference of IEEE India Council*, 2005, pp. 52–55.

[17] Y. Yu and H. Wu, "Anomaly Intrusion Detection Based Upon Data Mining Techniques and Fuzzy

Logic," in *IEEE International Conference on Systems, Man, and Cybernetics*, 2012, pp. 514–517.

[18] P. P. Chapke and R. R. Deshmukh, "Intrusion Detection System using Fuzzy Logic and Data Mining Technique," in *Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015) - ICARCSET '15*, 2015, pp. 1–5.

[19] M. Dixit and R. Ukarande, "Network Traffic Intrusion Detection System Using Fuzzy Logic and Neural Network," *International Journal of Synthetic Emotions*, vol. 8, no. 1, pp. 1–17, 2017.

[20] S. N. Pawar, "INTRUSION DETECTION IN COMPUTER NETWORK USING GENETIC ALGORITHM A PPROACH : A S URVEY," *International Journal of Advances in Engineering & Technology*, vol. 6, no. 2, pp. 730–736, 2013.

[21] P. G. Majeed and S. Kumar, "Genetic Algorithms in Intrusion Detection Systems: A Survey," *International Journal of Innovation and Applied Studies ISSN*, vol. 5, no. 3, pp. 2028–9324, 2014.

[22] A. N. Jaber, M. F. Zolkipli, S. Engineering, L. T. Razak, and O. Hanshal, "A CONCEPTUAL MODEL USING THE ELLIPTIC CURVE DIFFIE – HELLMAN WITH AN ARTIFICIAL NEURAL NETWORK OVER," in *The National Conference for Postgraduate Research*, 2016, pp. 534–540.

[23] N. Gupta, N. Pareek, and K. Pandey, "Genetic Algorithm based Network Intrusion Detection System," *International Journal of Advanced Research in Computer Science*, vol. 2, no. 6, pp. 480–484, 2011.

[24] S. N. Pawar and R. S. Bichkar, "Genetic algorithm with variable length chromosomes for network intrusion detection," *International Journal of Automation and Computing*, vol. 12, no. 3, pp. 337–342, 2015.

[25] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, "Network intrusion detection with Fuzzy Genetic Algorithm for unknown attacks," in *The International Conference on Information Networking 2013 (ICOIN)*, 2013, pp. 1–5.

[26] A. C. Enache and V. Sgârciu, "Designing Real-Time Anomaly Intrusion Detection Through Artificial Immune Systems," in *ECCWS2016-Proceedings for the 15th European Conference on Cyber Warfare and Security*, 2016, pp. 333–342.

[27] J. Shen and J. Wang, "Network intrusion detection by artificial immune system," in *IECON Proceedings (Industrial Electronics Conference)*, 2011, pp. 4716–4720.

[28] M. Tabatabaefar, M. Miriestahbanati, and J. C. Gregoire, "Network intrusion detection through artificial immune system," in *11th Annual IEEE International Systems Conference, SysCon 2017 - Proceedings*, 2017.

[29] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.