Intrusion detection systems based on Artificial Intelligence techniques

Sana R. Alkhaldi, Dr. Sabah M.Alzahrani
College of Computers and Information Technology , Taif University
Taif, Saudi Arabia
Email: S41181153@students.tu.edu.sa , sa.sabah@tu.edu.sa

Abstract:

Information technology is witnessing great development over time, and the use of computers and its various accessories such as printers, is spreading in various areas of life and for several purposes. And there has become a great necessity to connect computers through computer network technologies, whether local or global in the world, to exchange various data by sending them through networks, and this means that the computer is no longer alone in this environment, but must be located within a network, send and receive And he exchanges information with other devices, and this development has provided humanity with more facilities, but in return there has become a fertile field for criminals to practice their criminal activities, from here the concept emerged Informational crime. This paper will discuss this protection through the use of a branch of computer science called Artificial Intelligence AI. This survey is focused mainly on a task of intrusion detection by using Ml as sub-field from AI fields. We use Machine Learning (ML) at intrusion detection systems. Also, machine learning is not the only application of artificial intelligence that can be used, but there are several other applications.

Keywords: Cyber Crime, Artificial Intelligence (AI), Machine learning, intrusion detection systems (IDS), Intrusion Prevention System (IPS), Detection, Artificial Intelligence Application.

I. INTRODUCTION

Information technology is witnessing great development over time, and the use of computers and its various accessories such as printers, is spreading in various areas of life and for several purposes. With this development, methods of linking the computer and its accessories and between the account and other computers have evolved. And there has become a great necessity to connect computers through computer network technologies, whether local or global in the world, to exchange various data by sending them through networks, and this means that the computer is no longer alone in this environment, but must be located within a network, send and receive And he exchanges information with other devices, and this development has provided humanity with more facilities and amenities, but in return there has become a fertile field for criminals to practice their criminal activities, but this time it is not like what they do in normal life, but rather they will implement it electronically on devices and people, from here the concept emerged Informational crime. Also,

as continues development this technology, electronic crimes cases change. This technology also give a simple way to criminals to achieve goals of them, we are seen rising numbers and multi from electronic crimes each day. In addition, information technology simplify globalization for these electronic crimes by making that much hardest to monitoring, detecting, preventing or capturing information criminals and erasing borders of country [1], [2], [3]. It is increasingly used Information technology as tool to implement information crimes, criminals can commit easy and cheap crimes by a high-tech product and other eelectronic devices. Because all information system developed to Serving humanity like Internet, phones, computers are susceptible for criminal uses, we must protect them from risks.

This paper discusses this protection through the use of a branch of computer science called Artificial Intelligence AI, Artificial intelligence or machine intelligence appeared with the beginning of computers as scientific research field. Building hardware / software / systems smarter than humans at the beginning of artificial intelligence was "almost impossible" [4].

We can define AI as using the models of computational to study the faculties of mental. Research of AI contain basic fields such as knowledge representation, reasoning, scheduling and automated planning, ML, general intelligence, robotics and computer vision [5]. This survey is focused mainly on a task of intrusion detection by using Ml as sub-field from AI fields.

The most famous artificial intelligence interesting problem is under investigation intensive is ML, Learning is enhancement system of knowledge by reordering its base or extending or by enhancement the engine of inference [6].

We use Machine Learning(ML) at intrusion detection systems, IDS can be used to refer to Intrusion detection systems, its work idea done by monitoring system activities or network . One method of classifying IDS depended on the way of intrusion detection [5]. Also, we have another concept, It is IPS/IDPS or intrusion prevention system is an intrusion detection system which also has ability to preventation attacks. An IPS needs to detect attack at real time it also requires to preventing this attack. An IDS doesn't need to detect attack at the same moment it happens, although it is favored [5]. In addition to the use of machine learning in intrusion detection, we can evaluate it. Also, machine learning is not the only application of artificial intelligence that can be used, but there are several applications such as neural networks, intelligent agents, industrial immune system, genetic algorithms, and fuzzy logic.

This paper first of all, talks at second section about cyper crime as the great risk to all users of networks and devices at.

Third section shows the artificial intelligence or machine intelligence and how to use it at protecting Information. Fourth section talks about machine learning as a field of AI and use it to detect intrusion. Fifth section presents intrusion detection systems(IDS), and classification of it ,and it also shows Intrusion Prevention System and detection and this section will end with a mention the preferred characteristics of IDPS, Evaluating and Using ML for IDS will be present at 6the section. In the last two sections we will talk about others AI application to IDPS and advantages of AI application to IDPS.

II. CYBER CRIMES: OVERVIEW

There are lots of conveniences at our world and it has effective impact by computer and internet technology development, However, it has also passive impact like increase the problems that difficult to solve like the emergence of many forms of electronic crimes. For example, common electronic crimes like fraud and theft take new forms of “electronic Crimes” by information technology. Also, as continues development this technology, electronic crimes cases change. This technology also give a simple way to criminals to achieve goals of them, we are seen rising numbers and multi from electronic crimes each day.

In addition, information technology simplify globalization for these electronic crimes by making that much hardest to monitoring, detecting, preventing or capturing information criminals and erasing borders of country[1], [2], [3]. It is increasingly used Information technology as tool to implement information crimes, criminals can commit easy and cheap crimes by a high-tech product and other electronic devices. All information system developed to Serving humanity like Internet, phones, computers are susceptible for criminal uses. Typically, the target of crimes that use information technology system is email account, bank account, computer, server, website, personal information, and digital record of public and private institutions. "These crimes are also known as “Digital Crimes”, “Computer Crimes”, “Crimes of Information Technologies”, “Network Crimes” or “Internet Crimes”" [7].

Information crimes include offenses like computer intrusions, wrong use of intellectual rights, online exploitation, economic eavesdropping, laundering money, non-delivery of services or goods and other growing types of crimes facilitated by using Internet [1],[3],[8]. Although “information crimes” has been a famous phrase today, define it exactly is difficult. Most definitions existing are develop experimentally. Information crime defines as “any crime that is facilitated or committed using a computer, network, or International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 23 hardware device” where “computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime”[9].

Other definition for Information crime is “criminal activity or a crime that involves the Internet, a computer system, or computer technology” [10]. Information crime defines as “crime that occurs when computers or computer networks are involved as tool, locations, or targets of crime” [11]. While people communicate, shopping, working, sharing, communicating using Internet computer devices. The amounts of information processed and stored on computer devices and other systems of computing increases daily exponentially. The digital world brings together more people than ever before, place barriers and language have disappeared. Crimes and criminals concepts are present in real world, therefore virtual world has not remained separated from these concepts either [8]. “Most of the cyber crime we see today simply represents the migration of real-world crime to cyberspace which becomes the tool criminals used to commit old crimes in new ways " [12].

III. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence or machine intelligence appeared with the beginning of computers as scientific research field. Building hardware / software / systems smarter than humans at the beginning of artificial intelligence was "almost impossible"[13].

We can define AI as using the models of computational to study the faculties of mental. Research of AI contain basic fields such as knowledge representation, reasoning, scheduling and automated planning, ML, general intelligence, robotics and computer vision. This survey is focused mainly on a task of intrusion detection by using Ml as sub-field from AI fields. However, there are other methods than ML we will mention them. Dealing of ML with the algorithms study and construction that generalize (like learn) of restricted sets from data. These algorithms work by creating input-based models and then use them models to produce predictions or choices, instead of following specifically programmed instructions. Having this features makes them suitable candidates for the tasks of intrusion detection. ML attempts to solve three popular problems: regression, classification, and clustering. Regression involves predicting or estimating a response, classification means that group composition is established, whereas a collection from inputs is separated to groups in clustering, where all members have same characteristics. Based on the outputs, we're referring to classification when the outputs variable has class labels, when the outputs variable has continuous numeric value, we're referring to regression, while we're referring to clustering when the outputs variable are subsets. Regression can apply to prediction type from problems, rather than clustering and classification. Machine Learning categorized to three major groups, based on the methods of learning: reinforcement learning, unsupervised and supervised learning. At classification problems,

the widely used supervised learning, where the aim is to let the machine learn the systems of classification that we developed it. Unsupervised learning is even more difficult.

The aim is to make the machine learn how is doing thing without telling it how is doing it directly. It is an impressive tool that represents the properties of statistical to overall set of inputs patterns to recognize structures in nonlabelled data. Reinforcement learning will be carried out through contact with environments were through try and error, the agent of learning will be learned from the results of its acts rather than being directly instructed.

In order to maximize performance, we use several combined algorithms to get better reasoning efficiency than any single algorithm since we don't have a single algorithm at AI to achieve the best performance for all circumstances. In general there are two known approaches: hybrid and ensemble, hybrid approach combines completely heterogeneous different AI approaches, ensemble approach combines multiple weak but homogeneous models.using several merged algorithms commonly at the individual outputs level [5].

To solve difficult problems which need intelligence seem as human intelligence. A lot numbers from approaches have been improved in the field of artificial intelligence. Some from these approaches have achieved reach to maturity level because there are specific algorithms depend on these approaches. Even some approaches have become commonly known which they aren't longer relationship to AI, they become a subfield from some application, for example, algorithm which created from learning field of AI that named data mining. It is impossible to attempt to make full survey for all useful practically AI approaches in summarized survey. Rather than, we present machine learning as approach using it to respective approaches in cyber security defense[13].

IV. MACHINE LEARNINIG

The most famous artificial intelligence interesting problem is under investigation intensive is ML, Learning is enhancement system of knowledge by reordering its base or extending or by enhancement the engine of inference [6].Machine learning includes computational ways for new skill, getting new knowledge, and new methods to arrange existing knowledges. Learning problems are vary very by complexity of their from easy parametric learning that means learning parameter values, to complex forms from symbolic learning, such as, learn of grammars, functions, concepts, until learn behavior[14]. AI provides approaches for unsupervised learning and a supervised learning (learning by teacher). Unsupervised learning is beneficial in case of existence of huge quantity from data, and it is popular in cyber security because it can collect a lot of logs. Data mining appeared in origin from unsupervised learning field in AI. For neural nets, Unsupervised learning consider a functionality, Specifically, to self-organizing maps.

A distinguished type of learning approaches is comprised from algorithms of parallel learning which are appropriate for execution at parallel hardware.

Those learning approaches are performed by neural nets and genetic algorithms. For example, fuzzy logic and genetic algorithms are used, for systems of threats detection described at [15].

V. Intrusion Detection System (IDS):

The intrusion detection systems try to find intrusions of system, to confirm if the system is vulnerable to attack. Intrusions can be named anomalies or attacks, the abbreviation IDS can be used to refer to Intrusion detection systems, its work idea done by monitoring system activities or network. One method of classifying IDS depended on the way of intrusion detection[5]. Figure 1 shows IDS system:

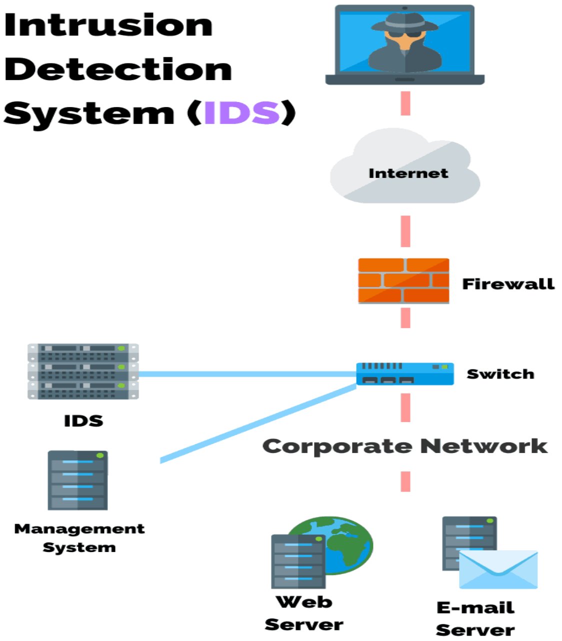


Fig. 1. Intrusion Detection System adapted to [16].

A. Host-Based Intrusion Detection System*:*

Intrusion detection systems that based on a host are systems which monitor the hardware that is install on it, or directly linked to. HIDS limited by logs of audit because they depend much on it.

The method they monitor the system start from the monitor the case of the basic system by logs of audit, to monitor execution of program. There is other issue is the huge size from logs of audit. Each log has monitored must be analyzed;

that means that HIDS can also have a large impact at the implementation on system of host when installed on it. Oher disadvantage is which any vulnerability which causes changing the files of audit, also affects the HIDS integrity. When audit log is replaced, the HIDS can't know and find that actually happened[5]. This type is shown in the figure 2.

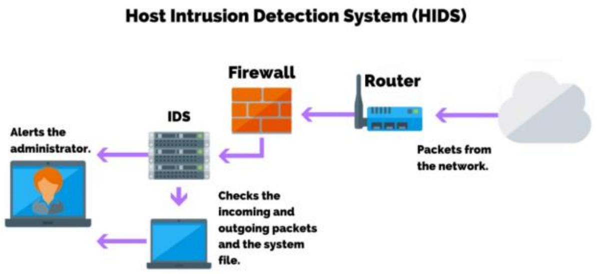

Host Intrusion Detection System (HIDS)
Firewall
Router
IDS
Alerts the administrator.
Packets from the network.
Checks the incoming and outgoing packets and the system file.

Fig. 2. Host Intrusion Detection System (HIDS) adapted to [16].

B. Network-Based Intrusion Detection System:

Intrusion Detection System based on Network, it placed within certain positions at a network for monitor traffic between devices inside the networks. They work by the same idea of wiretapping. By listening to communication which happens by "tap" at a network. The intruder will be attempt to reduce his activity at the network, but the risks are lower. NIDS are also more portable than HIDS. NIDS monitor the traffic within the network, and are separate from the operating systems they work on. The systems analyze the traffic by multiple approaches to determine if the malicious software are sending within data[5]. This type is shown in the figure 3.

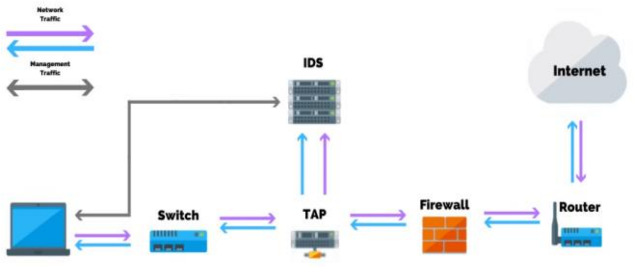


Fig. 3. Network Intrusion Detection System (NIDS) adapted to [16].

There are two several ways to analysis the data within network, Packet-based analyze and Flow-based analyze way. Packet-based analyze way uses the all packet involving the payload and headers. An intrusion detection system which uses packet-based analyze is named a packet-based network intrusion detection system. The benefit of this type of analyze is which there are large amounts of data to dial with.

Every unique byte from the packet will be used to determine if the packet contains malicious software or not. Flow-based analyze way doesn’t use single packets it uses general collected data on flows of network. An intrusion detection system which uses flow-based analysis is named a flow-based network intrusion detection system. A flow definition is a one communication between the hosts and other devices[5].

C. Intrusion Prevention System*:*

IPS/IDPS or intrusion prevention system is an intrusion detection system which also has ability to preventing attacks. An IPS needs to detect attack at real time it also requires to preventing this attack .An IDS doesn't need to detect attack at the same moment it happens, although it is favored. For networks attacks those prevention actions cause closing the communication, block IP or limit the data transmit. The changing require to detect attacks at real-time can strongly effect the approaches which are used for attacks detection. such as, IDS may give an alerts although it is uncertain that all alerted is a truly anomaly. An IPS must to be sure before it able take any action. Otherwise the IPS may take action that the business using the IPS doesn't need [5]. This system is shown in the figure 4.

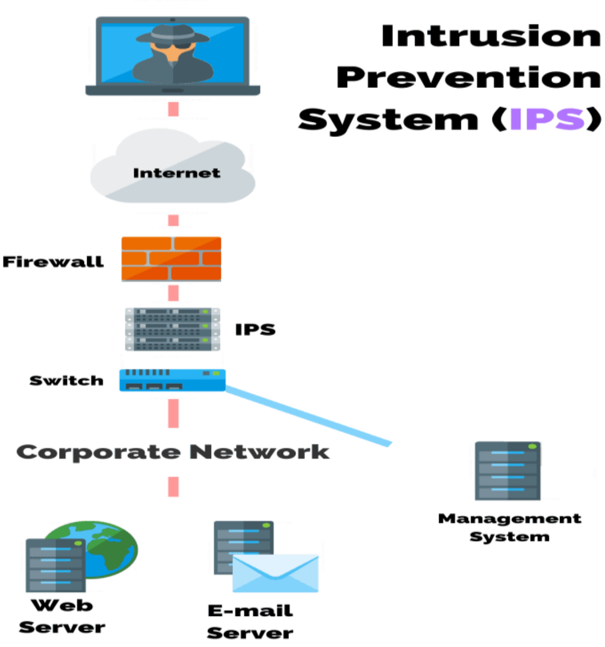


Fig. 4. Intrusion Prevention System (IPS) adapted to [16]

D. Detection*:*

Detection system has several different approaches to intrusions detection. They are methods depend on Signature and methods depend on Anomaly.

1) Methods depend on Signature *:*

At methods depend on Signature, The signature is compared to the stored signatures database .A flow or packet record is divide to features which all create a signature. If the packet or flow signature matches to any signature at the stored signature database, it will be classified as malicious. These approaches only compare the incoming signature with the stored signatures database and thus facilitate their deployment within the network, so they reduce overhead and pre-processing. It is not important for the system to know the traffic at the network. The database must be updated by new signatures, so that new attacks can be detected, since these methods are effective against previously known attacks. By simple modifying the signature, attackers can bypass the exact comparing these approaches provide it [5].

2) methods based on Anomaly*:*

Other name for this methods, methods based on behavior , they are approaches in that the IDS attempt to modeling behavior of traffic within network, When any of the packets received from the model is deviated, an alert must be sent to distinguish it as malicious. These methods must have the ability to distinguish any anomaly from correct behavior by using statistical models of correct behavior, Accordingly, there are new attacks being detected which deviate significantly from correct behavior. It is difficult to deploy a system in the network and at the same time we expect it to work, the system requires to know the traffic behavior o within the network, so it is necessary to create a model for the traffic within the network. If the data used for the training contains errors, such as classification errors, this causes many problems like generating false alerts positive . algorithms of Machine learning are used as one of the methods based on anomaly , Due to the ability of the techniques used in machine learning to learn from given data, so they can determine if the network has received malicious in data or not.

E. The preferred characteristics of IDPS*:*

There is specific characteristics of IDPS that are preferred to be available to achieve effective security against dangerous attacks. These characteristics are [17]:

- The ability to detect intrusion at real time, during or immediately after the actual attack.
- Minimize positive false alarms.
- Minimize supervision from Human to minimum, while ensuring continued operation.
- The ability to recover from system failures, whether due to attacks or accidental.
- The ability to Self-monitoring to detect attempts to tamper the system from attackers.
- Adhere to Security policy of system which IDPS monitors it.
- The ability to adapt with changes of system and behavior of user through time.

VI. Evaluating and Using ML for IDS

A. *Evaluating ML for IDS*

Performance is measured using an F-score by machine learning algorithms, This is however not enough to intrusion detection systems. Assuming The F-score that the same important is given to precision and recall. When the intrusion detection systems are evaluate, that is not actual case. A positive false occurs if a sample (model) is Normal actually but was distinguished as an Intrusion. A negative false occurs if a sample (model) is an Intrusion actually but was distinguished as Normal. A negative false is bad because it means there is no Intrusion was detected. Therefore, if Intrusion is not detected by any layer, the other layer detects it, using most intrusion detection systems IDS's in the multi-layer method. Multi-layer method might work in a different way. The first layer attempts to detect the largest number of anomalies (low recall), then passes the data in which it has detected anomalies to another layers. This method means which a low recall is not unacceptable. Using scoring for IDS which employs machine learning ML is depend on how using the IDS [5].

B. Using ML for IDS

Before using data at machine learning algorithms, it must be processed. That means, features must be selected, other features should be obtained by running tests and experimenting them, even if finding some features are easy. Better performance of IDS is not guaranteed. If all features of the dataset are used, there maybe It is not needed, or unhelpful for distinguishing between classes and thus increase the system error rate and computational costs [5].

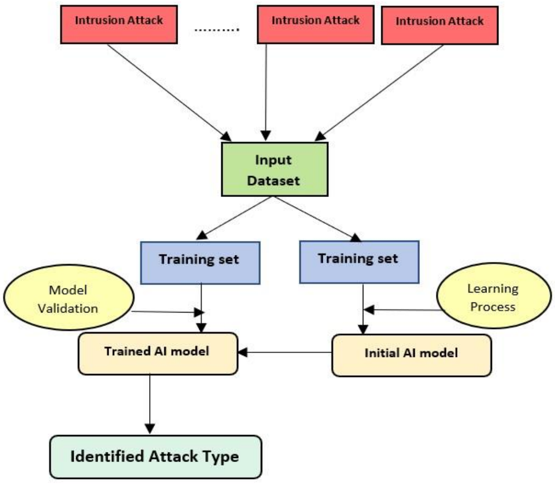


Fig. 5. Computational Intelligence Modeling Framework adapted [18].

VII. OTHERS AI APPLICATIONS TO IDPSs

Many of the current academic sources talk about the use of artificial intelligence applications in the fight against electronic crime. For example, Implement of many artificial intelligence techniques like data mining at anti-virus technique [19].

In the system of intrusion detection, neural network applications can be used to detect spam and “Denial of Service”(DOS) [20].

Intelligent agents can be used in some intrusion detection systems by sometimes combining them with technology of mobile agent [21].

Applications of the artificial immune system are used, which act as the natural immune system, and these technologies have become a basic role in cybersecurity [22].

Several models of the artificial immune system used in the intrusion detection system were analyzed, and the Danger Theory (DT) at the artificial immune system was presented as a way for responding to the danger in wireless networks [23].

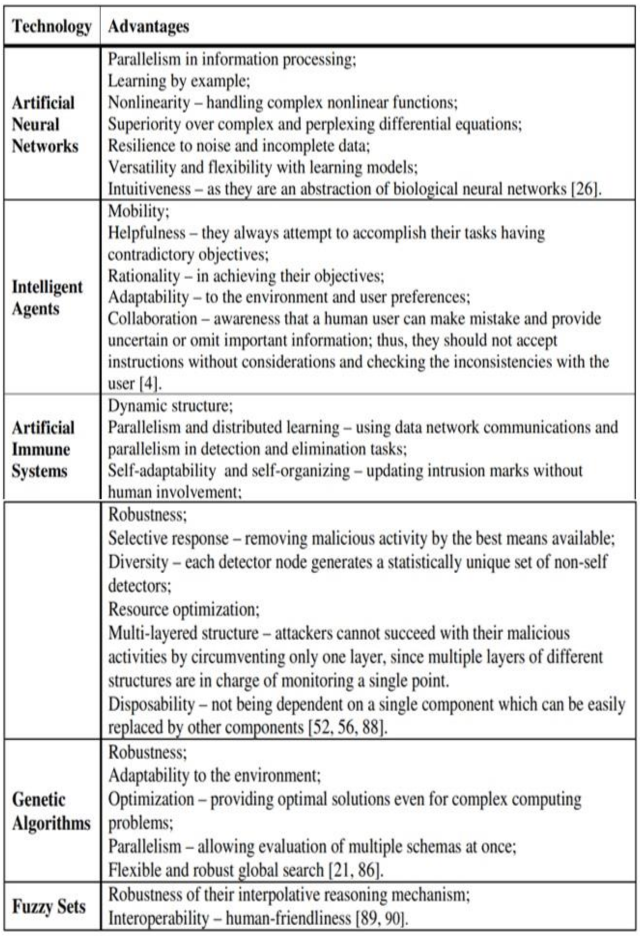
FIRE IDS have been developed, and they use techniques that extract data to process network data and reveal important metrics to detect the anomaly. This metrics is evaluated as a fuzzy set of each feature that has been observed and are used later to discover network threats [24].

An intrusion detection system based on a genetic algorithm has been introduced that monitors activities at a specific environment and determines if they are malicious or legitimate depending on the confidentiality and integrity of the system and the available data [25].

VIII.ADVANTAGES OF AI APPLICATIONS TO IDPSS

Artificial intelligence technologies provide multiple useful advantages for preventing and detecting intrusion, look at next table [7]:

Table 1. Advantages that some AI techniques bring to intrusion detection and prevention [7].



Technology	Advantages
Artificial Neural Networks	Parallelism in information processing; Learning by example; Nonlinearity – handling complex nonlinear functions; Superiority over complex and perplexing differential equations; Resilience to noise and incomplete data; Versatility and flexibility with learning models; Intuitiveness – as they are an abstraction of biological neural networks [26].
Intelligent Agents	Mobility; Helpfulness – they always attempt to accomplish their tasks having contradictory objectives; Rationality – in achieving their objectives; Adaptability – to the environment and user preferences; Collaboration – awareness that a human user can make mistake and provide uncertain or omit important information; thus, they should not accept instructions without considerations and checking the inconsistencies with the user [4].
Artificial Immune Systems	Dynamic structure; Parallelism and distributed learning – using data network communications and parallelism in detection and elimination tasks; Self-adaptability and self-organizing – updating intrusion marks without human involvement;
	Robustness; Selective response – removing malicious activity by the best means available; Diversity – each detector node generates a statistically unique set of non-self detectors; Resource optimization; Multi-layered structure – attackers cannot succeed with their malicious activities by circumventing only one layer, since multiple layers of different structures are in charge of monitoring a single point. Disposability – not being dependent on a single component which can be easily replaced by other components [52, 56, 88].
Genetic Algorithms	Robustness; Adaptability to the environment; Optimization – providing optimal solutions even for complex computing problems; Parallelism – allowing evaluation of multiple schemas at once; Flexible and robust global search [21, 86].
Fuzzy Sets	Robustness of their interpolative reasoning mechanism; Interoperability – human-friendliness [89, 90].

REFERENCES

1. Çakir, H. and E. Sert, *Bilişim Suçlari Ve Delillendirme Süreci.* Örgütlü Suçlar ve Yeni Trendler. OÖ Demir, M. Sever,(Eds.), Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010) Seçilmiş Bildirileri, Ankara: Polis Akademisi Yayınları, Ankara, 2011: p. 143.
2. Doğan, N., *Türkiye'de Bilişim Suçlarına Bakış.* Popüler Bilim, 2008. **8**(3): p. 14-17.
3. Poonia, A.S., A. Bhardwaj, and G. Dangayach. *Cyber Crime: Practices and Policies for Its Prevention*. in *The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management*. 2011.

4. Stampar, M. and K. Fertalj. *Artificial intelligence in network intrusion detection*. in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2015. IEEE.

5. Repalle, S.A. and V.R. Kolluru, *Intrusion detection system using ai and machine learning algorithm*. International Research Journal of Engineering and Technology (IRJET), 2017. **4**(12): p. 1709-1715.

6. Russell, P.N.S., *Artificial Intelligence: Modern Approach, Prentice Hall*. 2000.

7. Dilek, S., H. Çakır, and M. Aydın, *Applications of artificial intelligence techniques to combating cyber crimes: A review*. arXiv preprint arXiv:1502.03552, 2015.

8. DİJLE, H. and N. DOĞAN, *Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı.* International Journal of InformaticsTechnologies, 2011. **4**(2).

9. Gordon, S. and R. Ford, *On the definition and classification of cybercrime*. Journal in Computer Virology, 2006. **2**(1): p. 13-20.

10. http://dictionary.reference.com/browse/cybercrime. *cybercrime*. (24/11/2014).

11. Fisher, B.S., *Encyclopedia of victimology and crime prevention*. Vol. 1. 2010: Sage.

12. Brenner, S.W., *Cybercrime: criminal threats from cyberspace*. 2010: ABC-CLIO.

13. Tyugu, E. *Artificial intelligence in cyber defense*. in *2011 3rd International Conference on Cyber Conflict*. 2011. IEEE.

14. Ghosh, A.K., C. Michael, and M. Schatz. *A real-time intrusion detection system based on learning program behavior*. in *International Workshop on Recent Advances in Intrusion Detection*. 2000. Springer.

15. Hosseini, R., et al. *A genetic type-2 fuzzy logic system for pattern recognition in computer aided detection systems*. in *International Conference on Fuzzy Systems*. 2010. IEEE.

16. *https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/#NIDS*.

17. Patel, A., et al. *Autonomic agent-based self-managed intrusion detection and prevention system*. in *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*. 2011.

18. Anifowose, F.A. and S.I. Eludiora, *Application of artificial intelligence in network intrusion detection*. World Applied Programming, 2012. **2**(3).

19. Wang, X.-b., et al. *Review on the application of artificial intelligence in antivirus detection system i*. in *2008 IEEE Conference on Cybernetics and Intelligent Systems*. 2008. IEEE.

20. Chen, Y. *NeuroNet: towards an intelligent internet infrastructure*. in *2008 5th IEEE Consumer Communications and Networking Conference*. 2008. IEEE.

21. Herrero, Á., et al., *Hybrid multi agent-neural network intrusion detection with mobile visualization*, in *Innovations in Hybrid Intelligent Systems*. 2007, Springer. p. 320-328.

22. Rui, L. and L. Wanbo. *Intrusion response model based on AIS*. in *2010 International forum on information technology and applications*. 2010. IEEE.

23. Lebbe, M.A., et al. *Self-organized classification of dangers for secure Wireless Mesh Networks*. in *2007 Australasian Telecommunication Networks and Applications Conference*. 2007. IEEE.

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

25. Padmadas, M., et al. *Layered approach for intrusion detection systems based genetic algorithm*. in *2013 IEEE International Conference on Computational Intelligence and Computing Research*. 2013. IEEE.