International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

March 2023 Issue 54 Volume 15 Number 1 Pages 11-17

A REVIEW OF INTRUSION DETECTION SYSTEM METHODS AND TECHNIQUES: PAST, PRESENT AND FUTURE

Y.H. Alagrash [1] **H.S. Mehdy** [2] **R.H. Mahdi** [1]

1. College of Science, Computer Science Department, Mustansiriya University, Baghdad, Iraq
yhamza@uomustansiriyah.edu.iq, reyadh.hazim@mustansiriyah.edu.iq
2. College of Education, Computer Science Department, Mustansiriya University, Baghdad, Iraq
hala.shaker@uomustansiriyah.edu.iq

Abstract- The intrusion detection system (IDS) is a rapidly expanding field that continues to attract interest due to the increasing variety of its applications. It has been the topic of research, with a number of studies focusing on this issue and typically including cryptography. However, there are some assaults that cannot be thwarted using conventional methods. The likes of the Sybil attack, denial of service (DoS), black hole, etc., cannot be prevented by cryptographic methods. Nevertheless, the use of an Intrusion Detection System (IDS) can assist in detecting malicious activity and averting additional harm. This paper offers a Systematic Literature Review (SLR) that evaluates the viability of this solution type and highlight the future research directions. In addition, it should give details on the most prevalent methodologies, enabling the identification of the most prevalent machine learning (ML) algorithms, architectures, and datasets.

Keywords: Intrusion Detection System, Intelligent IDS, IDS Based on Machin Learning.

1. INTRODUCTION

Detecting intruders who seek to undermine the availability, confidentiality, or integrity of resources is the act of intrusion detection. It is used to safeguard the networks' systems. There is a prevalent misconception that firewalls detect and stop assaults by turning off everything and then reactivating only a few carefully selected objects [1]. As a complement to existing security measures, intrusion detection aims to catch behaviors that evade the safeguards monitoring and managing the system's content rather than replace prevention-based tactics like authentication and access control. There are two types of intrusion detection systems: host-based and network-based. an intrusion detection system based on the network gathers data by observing traffic on the network that the host is connected to, whereas an intrusion detection system based on host bases decisions on information and knowledge obtained from a single host [2]. Because of the importance of Intrusion detection systems (IDSs), it's possible to consider it as the second class after other protection mechanisms such that protection techniques and access control, Figure 1 illustrates an example of intrusion detection systems.

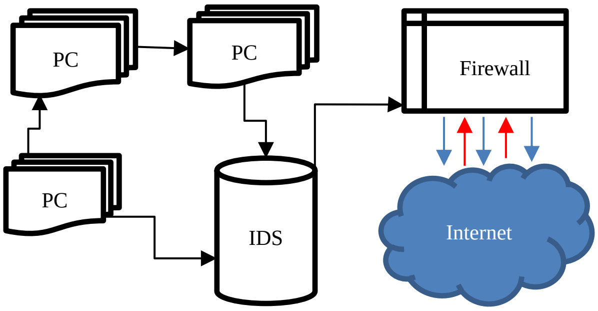

Figure 1. Example of IDS architecture

Data collection and analysis mechanisms deployed by current IDSs are quite varied. However, both approaches have two fundamental structural components: a detection module that gathers data that may include intrusion evidence and an analysis engine that evaluates this data to identify intrusion activities. Existing survey articles present a relatively narrow discussion on IDS, e.g., Vertma, et al. [3] have concentrated on network intrusion detection systems, whereas Bruno, et al. [4] discuss IDS in the internet of things. However, researchers and practitioners (especially newcomers to the field) must have a comprehensive grasp of IDS, including its fundamental concepts, research problems, application areas, and assessment approaches.

As IDS may be implemented in a variety of fields, there is a need for a comprehensive, field-agnostic reference covering the above IDS ideas. By comprehending the uses of agents in many fields, the reader will obtain useful insight into how to implement MAS. Understanding the open problems is useful for learning about possible hazards and limits, as well as for determining future research objectives. To comprehend the performance advantages that may be achieved with IDS and the possible tradeoffs, it is important to go into assessment methodology. Zeeshan, et al. [5] addressed the prominent characteristics of IDS and listed a handful of obstacles. However, they did not examine applications, assessments, and a larger range of obstacles, such as security and work distribution, among others.

In this article, we present a comprehensive introduction of IDS so that the reader may obtain a solid grasp of this expansive field. To do this, we will first define classical and detail their characteristics in order to clearly separate IDS definitions and structures. Next, a taxonomy of the uses and problems of IDS with artificial intelligence is presented. In addition, we explore the many methods used to assess the performance of IDS.

Figure 2 displays the section-by-section coverage of the major themes in this work, as well as the flow of ideas. The remainder of the review is structured as follows: Generic Intrusion detection system is introduced in Section 2. The third section explains MAS and their key characteristics, while the fourth section discusses MAS applications. The discussion in Section 5 is exhaustive.

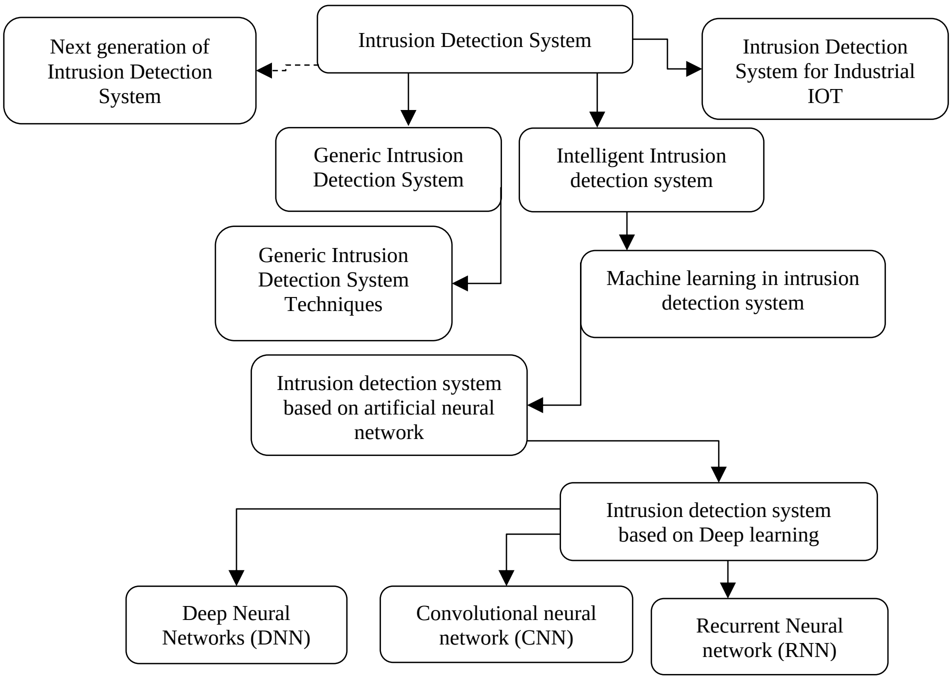
Intrusion Detection System
Next generation of Intrusion Detection System
Intrusion Detection System for Industrial IOT
Generic Intrusion Detection System
Intelligent Intrusion detection system
Generic Intrusion Detection System Techniques
Machine learning in intrusion detection system
Intrusion detection system based on artificial neural network
Intrusion detection system based on Deep learning
Deep Neural Networks (DNN)
Convolutional neural network (CNN)
Recurrent Neural network (RNN)

Figure 2. An overview of the paper

2.1. Generic Intrusion Detection System

The identification of numerous assaults and other harmful actions is an issue of signal detection [Inte02]. Therefore, intrusion detection is the detection of malicious system usage. To identify harmful system usage, we must differentiate between regular and malicious system use. There are now several techniques to solving this issue, as well as numerous intrusion detection systems. Numerous intrusion detection techniques rely on a model proposed by Dorothy Denning in 1987. This system is an autonomous system that is isolated from the platform, system sensitivity, and intrusion kind. This approach maintains a set of historically organized customer profiles, compares an observed file with the relevant file, updates the file if required, and then reports any found discrepancies [6].

In order to make decisions about whether security problems exist, some form of instrumentation must be provided by the system(s) being monitored. Event generator is the important part of the model that supports knowledge about the activities of the system. These Events are produced from system observation trials, from passage of internet, or from special application subsystem like firewall or authorization computers [7]. Sometimes in the literature, an event is defined as a higher-level abstraction than a primitive such as this file was opened. Contrarily, an activity profile allows you to monitor the computer's model or the internet's settings. The variables in the Activity Profile will be modified as a result of the data source's actions. The activities suggested by the rule set may generate new variables [8].

2.2. Generic Intrusion Detection System Techniques

In an effort to identify these intrusions automatically, software systems known as IDSs have been developed. They are based on the examination of certain behavioral patterns. These intrusions may be categorized into two primary detection patterns: Misuse assaults and Anomaly attacks. Misuse attacks are most popular intrusions on common lack views of a model and involve some of the hacking techniques described in the preceding section. Acquiring knowledge of system vulnerabilities that attackers seek to exploit is how abuse is modelled. This information is included into the intrusion detection system's rule set. This collection of rules serves as the foundation for intrusion detection. When an attack is in progress and data is sent to the intrusion detection system, the rule set is applied to the data to see whether any data sequences fit any of the rules. If a match is discovered, it indicates that a possible incursion is occurring. Utilizing expert systems to assess the data and apply the rule set is a common practice for misuse-based intrusion detection systems. This method is quite effective in detecting past assaults, but it is incapable of detecting new attacks because it is unaware of the patterns of new attacks. However, if the new assault is just slightly different from a previous attack, it may be able to identify it.

Anomaly attacks are depended on monitoring of perversions from natural model utilization patterns. They are discovered by constructing a file of the system being observed and discovering clear perversions from normal behavior. These calculations are calculated from obtainable system variables, like the mean of CPU storage, amount of network sessions through one minute, number of operations for customer, type of application accessed, etc. An anomaly, or deviation from a system profile, may be an indication of a possible intrusion.

The optimal approach may be a hybrid system that combines the pattern-matching profiles of an anomaly system with the caution of computer abuse detection software. Such a hybrid software might always monitor the model for anticipated assaults, but could overlook bogus false alarms if they originated from legitimate consumer behavior. Table 1 summarize the generic intrusion detect.

Table 1. Generic intrusion detection techniques

RF	Name Type	Description
[9]	Misuse IDS	Inspecting network traffic, misuse-based intrusion detection algorithms achieve low false positive rates (see Section V). In addition, they can successfully identify known assaults and mark them appropriately, which aids further investigation. However, there is one obvious flaw with misuse-based intrusion detection systems: Inability to identify unidentified and zero-day assaults. Other assaults that do not share parallels with recognized ones will go undiscovered due to their conditioning to identify known threats
[10]	Anomaly IDS	Anomaly techniques focus on behavior analysis to determine typical patterns by watching a series of occurrences. Nevertheless, it is erroneous to equate anomaly detection with behavior assessment, since signature-based approaches also include behavior evaluation. Due to its ability to recognize any deviation from the normal activities, this method can detect novel attacks and provide a customized model for the typical operations, reducing the likelihood that an attacker can conceal its movements and exert undue influence while still employing a conditional rule base
[11]	Hybrid IDS	The combination of anomaly and signature-based IDSs is regarded as a hybrid approach that delivers a better storage and computation cost tradeoff with fewer false positive alerts. Recently, the majority of systems are based on hybrid IDS owing to its efficient detection and straightforward operation
[12]	Adaptive IDS	As prospective methodologies, there have been some intriguing artificial intelligence-based techniques that exhibit flexibility. Learning Classifier Systems (LCS), Artificial Immune Systems, and Swarm Intelligence are examples of systems that integrate adaptability and evolution. However, this study field still faces several obstacles as systems and assault strategies grow increasingly complex

3. INTELLIGENT INTRUSION DETECTION SYSTEM

Emerging technology, connections, and breakthroughs have spawned several network structure dependencies. Increasing interconnectedness between enterprise apps necessitates an urgent focus on cybersecurity vulnerabilities. Typically, such intrusions have negative effects on corporate operations and result in large financial losses. Therefore, cybersecurity concerns are now a top focus for businesses. On the opposite end of the scale, advances in artificial intelligence and machine learning are helping researchers solve a wide range of issues:

3.1. Machine Learning in Intrusion Detection System

A Hybrid and Adaptive Intrusion Detection System developed by harnessing the advantages of Machine Learning methods to create a system that detects intrusions and warns the appropriate network administrator. This may also be expanded from intrusion detection to breach detection. The created system analyses and anticipates user behavior, which it then categorizes as either abnormal or normal.

Problems with machine learning may be broken down into the two types of supervised and unsupervised learning. ML algorithms are taught using pre-defined data in supervised machine learning. This data is initially tagged, and the system then learns and builds a model based on these tags. When fresh data is added to the model, the model is able to provide an accurate result. When it comes to learning, algorithms and training data are crucial. Also, under supervised machine learning, there are two main categories: regression and classification. Conveniently, the results of the hypothesis function may be found in the form of continuous spectrums in regression and discrete classes in classification [16]. Table 2 shows the summarize of classical machine learning that used widely in IDS.

Table 2. Machine learning in IDS

Approach	Description
support vector machine (SVM)	Support vector machines (SVM) are a class of supervised machine learning techniques that turn difficult, highly non-linear problems into binary classification models. To generate a hyperplane, the decision surface, and optimize the margin around it, the SVM needs data samples [13]
k-nearest neighbors' algorithm (KNN)	In both classification and regression, the k-nearest neighbor's algorithm (KNN) is a nonparametric technique. The K closest training instances in the feature space make up the input in both situations. Whether K-NN is applied for regression or classification determines the results: The outcome of a KNN classification is a class membership. A majority of an object's neighbors decide how to classify it, and the object is then put into the category that is most popular among its k closest neighbors (*k* is a positive integer, typically small). The object is simply assigned to the class of its one nearest neighbor if *k* = 1[14]
Random Forest (RF)	RFs are ensemble classifiers that are applied to the intrusion detection data for classification and regression analysis. In the training phase, RF creates several decision trees and outputs class labels that receive the majority of votes [12]. High classification accuracy is attained by RF, which also handles data noise and outliers. IDS uses RF because it is less prone to over-fitting and has a history of producing accurate classification results [15]

The machine learning concept of feature selection is implemented using a variety of techniques. Data mining, support vector machines, neural networks, and statistical analysis can all be used to choose attributes. As a consequence, three kinds of detection processes are assumed in feature selection: random, incremental, and decrement. In a dataset, the selection process is used to find and pick the most essential data points. For choosing features, a variety of methodologies are available, including the application of neural networks, deterministic algorithms, fuzzy and rough sets, intelligence patterns, and swarm intelligence. It is crucial to keep in mind as Table 3 based on [16].

Table 3. Most known malware features

RF	Feature	Categorization
[17]	Static	• File fingerprinting by hashing • Extraction of hard coded strings • Disassembly • Extract linked libraries and functions • Debugging
[18]	Dynamic	• Viewing Process Detail • File System activities monitoring • Registry activities monitoring • Network traffic monitoring
[19]	Data set	• Event triggered • Time triggered
[20]	Network traffic	• Duration • Source IP • Transport protocol • Destination IP address • Number of transmitted bytes • Number of transmitted packets • TCP flags

3.1. Intrusion Detection System Based on Artificial Neural Network

The functioning of real neurons in the brain and artificial neural networks were developed with the inspiration of the central nervous system. Artificial neurons in one or more hidden units are often used to weight and evaluate inputs to an ANN in order to ascertain the layer's output. A "learning rule" may be used to modify neurons in the hidden layer, output layer in an adaptive manner (usually gradient descent-based back-propagation of errors). ANNs are able to detect complicated and nonlinear relationships Because of their self-adaptive nature, they can distinguish between dependent and independent variables without the need for prior knowledge [21].

To classify data, ANNs have been applied in a vast array of situations and for a vast array of activities. For standard classification techniques like logistic regression and discriminant analysis, a thorough understanding of the underlying probabilistic model of the system that generated the data is necessary. A "black-box" methodology like an ANN, on the other hand, is more flexible than conventional classification methods since it can be tailored to the underlying model. As a result, they are especially valuable in areas like decision support for the identification of hidden weapons, Internet traffic forecasting and categorization, as well as the verification of signatures. Traditionally used classification methods like decision trees and k nearest neighbor algorithms are able to adapt to big dimensional datasets, which solves many model-building challenges [22].

Also in computer security, artificial neural networks (ANNs) have been used to analyses software design defects and identify computer viruses. Many other network threats may be successfully detected using ANN techniques, but their application to shellcode detection was not addressed [23].

3.2. Intrusion Detection System Based on Deep Learning

DL is a result of improvements in neural network (NN) algorithms (DL). Over a wide spectrum of research subjects, several techniques have been tried to overcome the restrictions of only having one hidden unit in NNs DL approaches. Object identification and picture categorization are two examples of applications of convolutional neural networks (CNNs). Learning feature hierarchies from enormous volumes of unlabeled data is one of the most powerful aspects of DL approaches. Network intrusion detection is a perfect application for DL techniques. Deep belief networks (DBNs), "restricted Boltzmann machines" (RBMs), and "supervised learning using convolutional neural networks" (CNNs)" are examples of deep learning (DL) methodologies, and "stacked Autoencoders (SAEs)" are increasingly being employed in networks. However, a multitude of hurdles and issues continue to plague network intrusion detection systems, preventing them from properly detecting irregularities [5].

First, the continual growth in attack volume and sophisticated threats causes an increase in network intrusion detection system false positives or false alarms (NIDSs). Second, a vast variety of network traffic types and a shortage of annotated training datasets are problems that "traditional machine learning (ML)" algorithms for network intrusion detection face [24]. These obstacles make it challenging to use typical ML approaches on big, real-world systems. In addition, traditional hand-crafted qualities are not easily accessible, versatile, or adaptable for growing complex methods.

Graphics processing units (GPUs), for example, are becoming more powerful pieces of computer hardware. As a method of feature extraction and a classifier, "machine learning (ML)" has been used to network intrusion detection in the past. The first kind use DL techniques discover or extract essential properties from unprocessed data. The second kind of categorization relies on extracted attributes. According to expert understanding, a distinctive feature is found. DL algorithms may be used to classify data using extracted features.

3.2.1. Convolutional Neural Network (CNN)

Self-optimization via learning neurons is the same as that of classic ANNs in the CNN process. Nonlinear functions serve as the foundation for innumerable ANNs, and each neuron will carry out an action and receive input.

The following is how CNNs are employed. Detection of cyber-attacks by use of hardware: Because users aren't allowed to wear helmets while using ATMs, this plan was presented as a CNN strategy for safeguarding the machines. This was accomplished via the use of Google's inception concept. Automated helmet detection may be improved greatly by using ATM surveillance video feed. While being trained on a confidential ATM surveillance dataset, the model attained an accuracy rate of 95.3% [25].

3.2.2. Recurrent Neural Network (RNN)

Unlike other techniques, this one has a unique characteristic that mirrors the human brain's thought process. The approach is appropriate for handling real-time learning tasks because it can handle time-series data, and hence accomplish difficult tasks, such as unsegmented and pattern recognition [26]. Articles using RNNs as a DL approach are listed as follow.

Based on RNN classification, an IDS has been presented in [30]. For binary and multiclass classification, several hidden node counts and learning rates were used in the studies. In order to get a realistic performance, this technology required considerable computational processing. According to [27], intrusion detection was proposed of have suggested DL-based detection of distributed denial of service (DDoS) attacks.

Intruder behavior detection: According to [27], In an effort to forecast user behavior on Tor networks, a research team used deep RNNs in conjunction with kernel PCA, long short-term memories. The recommended threat analysis method performed better than previous methods. In a separate investigation, an approach for intruder analysis and identification employing DL networks and association rule mining was devised. Foresee potential intruder activities and the locations where they may come from, and then depict the course of intruder attacks.

3.2.3 Deep Neural Networks (DNN)

DNNs, which offer potent tools for automatically producing high-level abstractions of complicated multimodal data, have lately garnered a great deal of interest from business and academics. A growing number of studies have indicated that deep neural networks (DNNs) are more efficient and trustworthy than shallow neural networks [28].

Attack detection: According to the authors [28], IOT systems have a high-level feature extraction capability that may be a durable defense against fresh attacks or minor modifications. In order to find hidden patterns in training data, the ability to compress data, as well as the self-taught DL architecture, are critical for distinguishing malicious from benign traffic. To solve this problem, the authors [29] propose a DNN with 41 features and three hidden layers. Those who concentrated on a lot of courses were less accurate. The authors of [29] looked at fault injection attacks on DNNs. By altering DNN parameters using a defect injection approach, attackers incorrectly identified a certain input pattern as hostile. These goals were met by presenting two types of fault injection attacks by the authors.

3.3. Merits and Limitations of Intelligent Intrusion Detection System

Companies may experience crippling problems as a result of security breaches, including circumstances that are impossible to recover from. Although intrusion detection systems can help with cybersecurity challenges, they are challenging to implement. False positive rates for anomaly-based intrusion detection systems are frequently quite high and are computationally intensive.

The majority of traditional machine learning research has concentrated on models, optimizers, and computational difficulties. As technological development and hardware improvements alleviate these obstacles, practitioners are discovering that their datasets are the source of their models' limits and flaws. This is especially true for deep networks, which often depend on enormous datasets that are too vast and cumbersome for domain experts to manually moderate (Table 4).

Table 4. Merits and limitations of IDS

Merits	Limitations
• Anomaly IDS • Distributed architecture: IDS design approaches that depend on local knowledge and datasets benefit from the distributed nature of the generation • Edibility is provided by IDS in a number of ways, including "plug and play" system updates and a range of agents that mimic heterogeneous sources and loads • Complexity and real time system	• This is owing to the shortcomings of classical IDS, which include inaccurate categorization of network abnormalities as attacks, a poor rate of attack detection, and a high percentage of false positives among detected assaults • Portability: It may be challenging to implement speculative IDS concepts and architectures on hardware • Scalability: With today's computer power, researchers can simulate bigger micro-grids by coordinating the behaviors of several individuals on a single computing platform

4.1. Intrusion Detection System for Industrial IOT

Even though it is based on regular laws, the traditional IDS is ineffective at identifying aberrant patterns. These rules cannot be modified in smart homes by introducing new anomalous patterns. As a result of the many security risks that smart home devices and networks face, machine learning is increasingly being seen as a viable option for securing them. Because diverse techniques for training sensors and computers don't need any explicit programming on the user's part, machine learning may take use of artificial intelligence [30].

Manipulation of information to control industrial activities poses the greatest hazard to IIoT, since it might seriously disrupt operations and put people's lives in peril. To deal with these problems, it's possible that current solutions fall short. When it comes to the Internet of Things (IIoT), security measures such as firewalls, access control, and encryption are not adequate. The first issue is that IIoT systems are very sensitive to cyber-attacks since they manage and monitor real-time events that create large amounts of aggregated data from scattered network nodes that are processed by a centralized curator [40].

This includes signature-based (or knowledge-based), anomaly-based, and specification-based detection. This kind of IDS uses signatures or machine learning algorithms to compare and discover abnormalities, which are the most popular ways. Although they have shown to be quite effective in stopping cyber assaults, they suffer from either an inability to identify zero-day attacks as in signature-based or high false positive alarms as in anomaly-based systems [41]. A simple IDS, however, is no longer adequate to defend a network from increasingly complex and sophisticated attacks. Since multiple IDS nodes gather and exchange information with each other, collaborative intrusion detection systems (CIDS) are established, resulting in greater efficiency and performance. Detecting intrusions is complicated by the need to integrate many tools.

5. NEXT GENERATION OF INTRUSION DETECTION SYSTEM

An integrated security management panel that contains software for intrusion detection. With the integrated "host intrusion detection" (HIDS), "network intrusion detection" (NIDS), and "cloud intrusion detection" (CID) technologies, you will be able to spot attacks on your essential on-premises and cloud infrastructure as soon as they happen based on the following:

- Use host-based, network, and cloud IDS built-in to detect intrusions in any environment.
- Quickly use the Kill Chain Taxonomy figure out what a threat wants and how it plans to do it.
- Use contextual information regarding assaults, such as a description of the danger, its technique and strategy, and recommended responses, to make educated judgments.
- Utilize automated alerts so that you are alerted of significant hazards as they occur.
- Work more productively with powerful analytics that offer detailed information on threats and vulnerabilities - all from a single interface.

6. CONCLUSION

In this survey, we proposed a high-level, all-encompassing discussion of various aspects of IDS, which assists newcomers in understanding the fundamental concepts of IDS, existing applications in a variety of disciplines, the challenges of developing IDS, and the methods for analyzing IDS performance. First, we defined agents and IDS and detailed their main characteristics. Then, we explored the main uses and problems of IDS while providing resources for more research. Following a study of agent-to-agent interactions, the article concludes with a discussion of evaluation techniques for analyzing the success of an agent-based system. We hope that scholars and people who work in the field will use this paper as a complete and useful reference on IDS.

REFERENCES

[1] S. Jin, J.G. Chung, Y. Xu, "Signature-Based Intrusion Detection System (IDS) for in-Vehicle can Bus Network", IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5, 2021.

[2] M. Liu, Z. Xue, X. Xu, C. Zhong, J. Chen, "Host-Based Intrusion Detection System with System Calls: Review and Future Trends", ACM Comput. Surv., Vol. 51, No. 5, pp. 1-36, 2019.

[3] J. Verma, A. Bhandari, G. Singh, "Review of Existing Data Sets for Network Intrusion Detection System", Adv. Math. Sci. J., Vol. 9, No. 6, pp. 3849-3854, 2020.

[4] B.B. Zarpel Ao, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, "A Survey of Intrusion Detection in Internet of Things", J. Netw. Comput. Appl., Vol. 84, No. September 2016, pp. 25-37, 2017.

[5] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches", Trans. Emerg. Telecommun. Technol., Vol. 32, No. 1, pp. 1-29, 2021.

[6] S. Shamshirband, M. Fathi, A.T. Chronopoulos, A. Montieri, F. Palumbo, A. Pescape, "Computational Intelligence Intrusion Detection Techniques in Mobile Cloud Computing Environments: Review, Taxonomy, and Open Research Issues", J. Inf. Secur. Appl., Vol. 55, No. August, pp. 1-51, 2020.

[7] J. Enrique, R. Cortes, "Analysis and Design of Security Mechanisms in the Context of Advanced Persistent Threats Against Critical Infrastructures", Ph.D. Thesis, Malaga University, pp. 1-310, Spain, 2022.

[8] M. Botacin, et al., "AntiViruses under the Microscope: A Hands-on Perspective", Comput. Secur., Vol. 112, No. i, pp. 1-84, 2022.

[9] D. Papamartzivanos, F. Gomez Marmol, G. Kambourakis, "Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems", IEEE Access, Vol. 7, pp. 13546-13560, 2019.

[10] Y. Alagrash, N. Mohan, S.R. Gollapalli, J. Rrushi, "Machine Learning and Recognition of user Tasks for Malware Detection", The 1st IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. (TPS-ISA), No. February 2020, pp. 73-81, 2019.

[11] A. Golrang, A.M. Golrang, S.Y. Yayilgan, O. Elezaj, "A Novel Hybrid IDS Based on Modified NSGAII-ANN and Random Forest", Electron., Vol. 9, No. 4, pp. 1-19, 2020.

[12] E. Anthi, L. Williams, P. Burnap, "Pulse: An Adaptive Intrusion Detection for the Internet of Things", IET Conf. Publ., Vol. 2018, No. CP740, pp. 1-4, 2018.

[13] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, T. Huang, "A Real-Time and Ubiquitous Network Attack Detection Based on Deep Belief Network and Support Vector Machine", IEEE/CAA J. Autom. Sin., Vol. 7, No. 3, pp. 790-799, 2020.

[14] K. Taunk, "A Brief Review of Nearest Neighbor Algorithm for Learning and Classification", Int. Conf. Intell. Comput. Control Syst. (ICCS 2019), pp. 1255-1260, 2019.

[15] Y. Alagrash, A. Drebee, N. Zirjawi, "Comparing the Area of Data Mining Algorithms in Network Intrusion Detection", J. Inf. Secur., Vol. 11, No. 01, pp. 1-18, 2020.

[16] S. Maza, M. Touahria, "Feature Selection Algorithms in Intrusion Detection System: A Survey", KSII Trans. Internet Inf. Syst., Vol. 12, No. 10, pp. 5079-5099, 2018.

[17] H. Alazzam, A. Sharieh, K.E. Sabri, "A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer", Expert Syst. Appl., Vol. 148, p. 113249, 2020.
[18] M. Wang, Y. Lu, J. Qin, "A Dynamic MLP-Based DDoS Attack Detection Method using Feature Selection and Feedback", Comput. Secur., Vol. 88, p. 101645, 2020.
[19] I.F. Kilincer, F. Ertam, A. Sengur, "Machine Learning Methods for Cyber Security Intrusion Detection: Datasets and Comparative Study", Comput. Networks, Vol. 188, No. October 2020, p. 107840, 2021.
[20] N. Yoshimura, H. Kuzuno, Y. Shiraishi, M. Morii, "DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic", Sensors, Vol. 22, No. 12, p. 4405, 2022.
[21] A. Shenfield, D. Day, A. Ayesh, "Intelligent Intrusion Detection Systems using Artificial Neural Networks", ICT Express, Vol. 4, No. 2, pp. 95-99, 2018.
[22] A. Bellat, K.H. Mansouri, A. Raihani, "Implementation of Artificial Neural Network for Optimization of a Wind Farm", Int. J. Tech. Phys. Probl. Eng., Vol. 13, No. 2, pp. 35-39, 2021.
[23] A. Shalaginov, S. Banin, A. Dehghantanha, K. Franke, "Machine Learning Aided Static Malware Analysis: A Survey and Tutorial", Adv. Inf. Secur., Vol. 70, No. 1, pp. 7-45, 2018.
[24] Y.H. Su, M.C.Y. Cho, H.C. Huang, "False Alert Buster: An Adaptive Approach for NIDS False Alert Filtering", ACM Int. Conf. Proceeding Ser., pp. 58-62, 2019.
[25] M. Asam, et al., "Malware Classification Using Deep Boosted Learning", arXiv Prepr. arXiv, pp. 1-23, 2021, https://arxiv.org/abs/2107.04008.
[26] A. Elomari, L. Hassouni, A. Maizate, "Deep Learning for Optimization of Chunks Placement on Hadoop/HDFS", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 49, vol. 13, No. 4, pp. 194-200, December 2021.
[27] F. Meng, Y. Fu, F. Lou, "A Network Threat Analysis Method Combined with Kernel PCA and LSTM-RNN", The 10th Int. Conf. Adv. Comput. Intell. (ICACI), pp. 508-513, 2018.
[28] A. Derhab, A. Aldweesh, A.Z. Emam, F.A. Khan, "Intrusion Detection System for Internet of Things Based on Temporal Convolution Neural Network and Efficient Feature Engineering", Wirel. Commun. Mob. Comput., Vol. 2020, No. April, pp. 1-16, 2020.
[29] M. AL Shabi, "Design of a Network Intrusion Detection System using Complex Deep Neuronal Networks", Int. J. Commun. Networks Inf. Secur., vol. 13, No. 3, pp. 409-415, 2021.
[30] I. Tarimer, S. Eren, "An IoT Application with Particle Card over Cloud", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 36, Vol. 10, No. 3, pp. 6-13, September 2018.

BIOGRAPHIES

Name: **Yasamin**
Middle Name: **Hamza**
Surname: **Alagrash**
Birthday: 11.06. 1978
Birth Place: Baghdad, Iraq
Bachelor: Computer Science and Statistical, Alrafedian University College, Baghdad, Iraq, 1999
Master: Data Security, Computer Science Department, University of Technology, Baghdad, Iraq, 2003
Doctorate: Cyber Security, School of Engineering and Computer Science, Computer Science and Informatic Department, Oakland University, MI, USA, 2020
The Last Scientific Position: Lecturer, Computer Science Department, College of Science, Mustansiriyah University, Baghdad, Iraq, 2012
Research Interests: Cyber Security, Artificial Intelligent, Malware Detection
Scientific Publications: 22 Papers, 2 Theses
Scientific Memberships: Iraqi IEEE

Name: **Hala**
Middle Name: **Shaker**
Surname: **Mehdy**
Birthday: 23.05.1981
Birth Place: Baghdad, Iraq
Bachelor: Computers Science, Computer Collage and Information Technology, Anbar, Iraq, 2004
Master: Computer Science, South Federal University, Rostov, Russia, 2017
The Last Scientific Position: Lecturer, Computer Science Department, Education Collage, Mustansiriyah University, Baghdad, Iraq, 2009
Research Interests: Artificial Intelligent, Image Process, Data Security
Scientific Publications: 3 Papers, 1 Theses

Name: **Reyadh**
Middle Name: **Hazim**
Surname: **Mahdi**
Birthday: 19.09. 1972
Birth Place: Baghdad, Iraq
Bachelor: Computer Science, Computer Science Department, Education College, Mustansiriyah University, Baghdad, Iraq, 2002
Master: Information Security, Information Technology Department, Art and Science, Utara University, Malaysia, 2009
The Last Scientific Position: Lecturer, Computer Science Department, College of Science, Mustansiriyah University, Baghdad, Iraq, 2013
Research Interests: Data Security, Artificial Intelligent, Machine Learning
Scientific Publications: 14 Papers, 1 Theses