# Intrusion Detection System Techniques: A Review

**Omar Fitian Rashid*[1], Noor Thamer Mahmood[2], Zahraa A. H. Alobaidy[3]**

[1] Department of Computer Technology Engineering, Al-Hikma University College, Baghdad, Iraq

[2]Department of Computer Science, Mustansiriyah University, Baghdad, Iraq

[3] Collage of Science for Women, University of Baghdad, Baghdad, Iraq

*Corresponding author: omaralrawi08@yahoo.com

## Abstract

With the high usage of computers and networks in the current time, the amount of security threats is increased. The study of intrusion detection systems (IDS) has received much attention throughout the computer science field. The main objective of this study is to examine the existing literature on various approaches for Intrusion Detection. This paper presents an overview of different intrusion detection systems and a detailed analysis of multiple techniques for these systems, including their advantages and disadvantages. These techniques include artificial neural networks, bio-inspired computing, evolutionary techniques, machine learning, and pattern recognition.

***Keywords:***Anomaly; Artificial neural networks; Bio-inspired computing; Intrusion detection; Misuse

## 1. Introduction

Security plays an important role in using computer networks by people and companies is getting more widespread [1]. Firewall and antivirus are examples of computer security types, and these systems are routinely used in the current days. Antivirus is computer software that prevents, detects, and removes malicious software and malware that may be viruses, Trojan horses, worms, and spyware based on known signatures stored in their database. The main problem is that most antiviruses programs update their signatures weekly or daily, which may expose computer users to new intrusion during the intervals between updates. On the other hand, a Firewall is a system used to monitor and control incoming and outgoing network traffic based on some security rules [2]. The primary defect of the firewall system, it can prevent external intrusion only. This encourages companies to build their monitoring system that is used to monitor data flow in their network. These systems are called IDS. IDS is used to recognize the unauthorized user and misuse of computer systems and networks. [1].

These systems have many advantages, such as detecting internal and external attackers, providing an easy protection system for the entire network, providing centralized management, and providing an additional layer of protection. On the other hand, IDS disadvantages: generate many alarms (false alarms) that lead to increased analysis workload, requiring high performance, and a large training data needed to characterize normal behaviour patterns.

## 2. Intrusion Detection Methods

Intrusion detection can classify into two methods: the first method is misuse (signature-based), and the second method is anomaly (behaviour based). Misuse intrusion detection is used a predefined attacks pattern that takes advantage of system weaknesses and application software to distinguish the intrusions. Where misuse systems discover intrusions based on malicious activity patterns, these systems can detect known attacks accurately. The comparison is made between available signatures and the network activities or between known signatures and system activities, and the missing report rate is high [3].

On the other hand, anomaly intrusion detection is based on normal usage behaviour patterns to distinguish the intrusions. The training is done by using traffic normal behaviours patterns. After that, distinguish malicious activity based on its variation from the normal behaviour and report it as attacks. Anomaly systems can detect unknown intrusions, and the missing report rate is low [3].

These intrusion detection methods (misuse and anomaly) have their advantages and disadvantages, where the advantages and disadvantages of both detection methods are listed in Table 1.

**Table 1- Advantages and disadvantages of intrusion detection methods**

| Method | Advantages | Disadvantages |
|---|---|---|
| Misuse Detection | **1.** Can detect attacks accurately<br>**2.** Create a lower false alarms rate. | **1.** Cannot detect new attacks. |
| Anomaly Detection | 1. Can detect new attacks.<br>2. Can detect abuse of privileges. | **1.** Create a high false alarm rate.<br>**2.** In the training phase may not cover all behaviour scope.<br>**3.** The change of user behaviour with time lead to decreased system performance. |

Several kinds of research were proposed based on hybrid IDS, where a hybrid intrusion detection

combines the strength of both techniques and tries to bypass their weaknesses, leading to enhanced IDS performance.

## 3. IDS Techniques

IDS has become one of the most discussed network security topics in the last few years. The first IDS method was built to monitor the computer systems security, and this method was done periodically. Since that time, different techniques have been proposed for IDS. These techniques are artificial neural network (ANN), bio-inspired computing, evolutionary technique, machine learning, and pattern recognition. The categorization of these techniques is shown in Fig. 1 below.

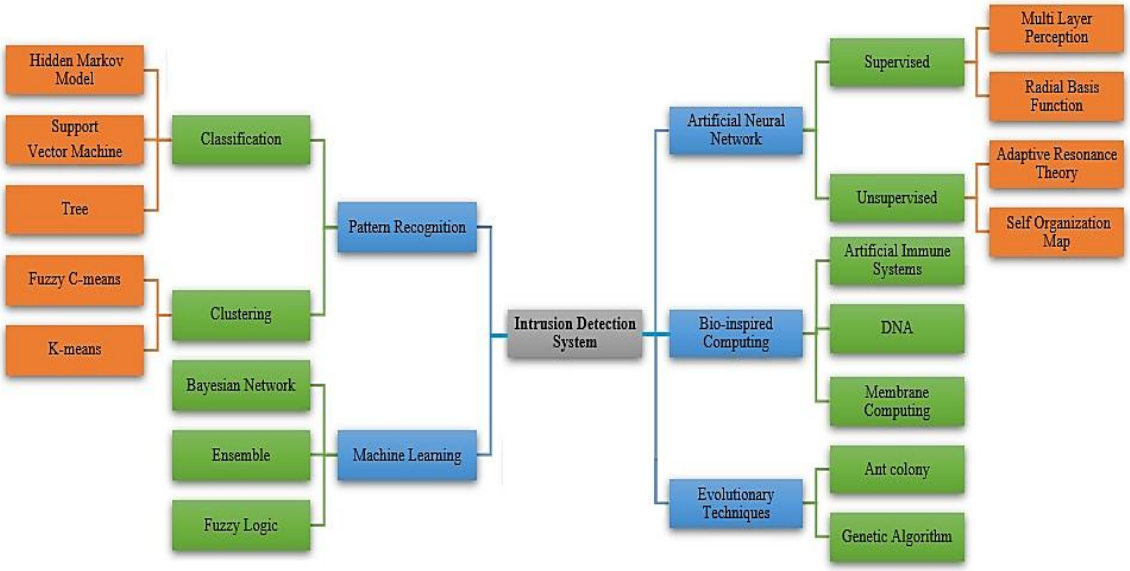


**Figure -1 IDS Techniques**

### 3.1 Artificial Neural Networks for IDS

ANN is a model used to process information inspired by the biological nervous systems, such as the brain. This is done by representing the thinking process by an electronic circuit or software. These systems consist of individual neurons, and each neuron (neural network) performs as a separate processing element. The output of each neuron is used as input to the neurons in the next layer. [4].

A NN has been utilized in different fields such as medicine, biology, engineering, and others. ANN is used to find a solution for some problems. One of these problems is a pattern recognition problem. One of the first attempts that used ANN for IDS was made by building an offline IDS for ten users using three layers architecture, and this system was proposed by Ryan et al. [5]. Some

disadvantages of applying ANN for IDS, the training time for this method is slow, making it not suitable for real-time, and when a new attack is added, the whole system must be retrained.

Various studies have been proposed for IDS based on ANN, either based on one ANN method or a combination of two ANN methods. Table 2 shows the reviews of some IDS using the ANN technique.

**Table 2- Reviews for some IDS based on ANN techniques**

| Author(s) | Year | Method(s) | Detection Methodology | Dataset | Performance |
|---|---|---|---|---|---|
| Haddadi et al. [6] | 2010 | Feed-forward neural network | - | KDDCup 99 | DR:<br>Normal = 79.8%,<br>DoS = 97.5%<br>Probe = 99.1%<br>R2L = 98.9%<br>U2R = 34.5% |
| Wang & Yu [7] | 2013 | Radial basis Functions and Elman | Hybrid | 1998 DARPA | Anomaly:<br>DR = 93%<br>FAR = 2.3%<br>Misuse:<br>DR = 95.3%<br>FAR = 1.4% |
| Xing-zhu [8] | 2016 | Radial basis Functions | - | KDDCup 99 | DR:<br>DoS = 95.80%<br>Probe = 93.95%<br>R2L = 95.20%<br>U2R= 96.02% |
| Chun et al. [9] | 2017 | Neural Network | - | NSL-KDD | DR:<br>DoS = 82.39%,<br>Probe = 81.16%<br>R2L = 20.8% |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Accuracy = 80.34% |
| Kim et al. [10] | 2017 | Deep Neural Network | - | KDDCup 99 | DR = 99% Accuracy = 99% FAR = 0.08% |
| Shenfield et al. [11] | 2018 | Artificial Neural Network | - | - | Accuracy = 98% Precision = 97% Sensitivity = 95% |
| Singh et al. [12] | 2021 | Deep Neural Network | - | UNSW2015 | Accuracy = 99% |

3.2 Bio-inspired Computing for IDS

Computers and organisms have a huge similarity. Bioinformatics used information technology to model biological processes. This method has helped find similarities more accurately and can be used in computer security [13]. IDS problems can be solved based on Bio-inspired such as Immune Systems, DNA, and Membrane Computing.

The human body uses a natural immune system to defend against harmful foreign cells (antigens) such as bacteria and viruses [14]. The artificial immune system was designed based on human immune system ideas such as diversity, error tolerance, dynamic learning, adaption, and self-monitoring [15]. Computer security uses the immune system based on classical theory [16] that is considered a measure for IDS.On the other hand, any computer system can be represented based on DNA characterization (DNA sequences or genes) [17], such as network traffic, system calls, and user behaviour. DNA was applied in several computer system domains such as cryptography, steganography, digital signature, etc.

Finally, another bio-inspired branch is membrane computing, where these systems extract computing models from the structure and functioning of living cells or other higher-order structures [18]. Table 3 shows the reviews of some IDS using Bio-inspired methods.

**Table 3- Reviews for some IDS based on bio-inspired methods**

| Author(s) | Yea | Method(s) | Detection | Dataset | Performance |
|---|---|---|---|---|---|

| | **r** | | **Methodology** | | |
|---|---|---|---|---|---|
| Al-Ibaisi et al. [19] | 2008 | DNA sequence encoding and Genetic algorithm | Anomaly | KDDCup 99 | DR:<br>DoS = 51.83%<br>Probe = 57.28%<br>R2L = 24.20%<br>U2R = 43.10 |
| Zhang et al. [20] | 2011 | Artificial Immune System | Anomaly | NSL-KDD | DR:<br>Normal = 96%<br>DoS = 96.04%<br>Probe = 89.8%<br>R2L = 99.7% |
| Randrianasolo & Pyeatt [21] | 2012 | Artificial Immune System and Holland's classifier | - | - | DR = 90.57%<br>False Positive Rate = 17.21%<br>False Negative Percentage = 9.42% |
| Idowu et al. [22] | 2013 | Membrane Computing | Anomaly | KDDCup 99 | DR = 80.62%, 93.07%, and 93.63%. FAR = 0.009%, 0.001%, and 0.001%. |
| Hameed & Rashid [23] | 2014 | DNA sequence encoding | Misuse | KDDCup 99 | Based on keys only:<br>DR = 99%<br>FAR = 27.2%<br>Accuracy= 94.4% |
| Hosseinpour et al. [24] | 2014 | Artificial Immune System | Anomaly | KDDCup 99 | FPR = 0.8%<br>TNR = 99.1%<br>Accuracy = 77.1% |
| Idowu et al. [25] | 2014 | Membrane Computing | Anomaly | KDDCup 99 | DR = 89.11%<br>FAR = 0.004% |
| Rashid et al. [26] | 2017 | DNA sequence | Anomaly | KDDCup 99 | DR = 86.36%<br>FAR = 49.69% |

| | | | | | |
|---|---|---|---|---|---|
| | | encoding | | | Accuracy = 77.65% |
| Farahnakian & Heikkonen [27] | 2018 | Deep Auto Encoder | Anomaly | KDDCup 99 | DR = 95.65%<br>FAR = 0.35%<br>Accuracy = 96.53% |
| Suliman et al. [28] | 2018 | Artificial Immune Systems and | - | KDDCup 99 | True Positive rate based on different probability values = 97.02%, 98.48%, and 99.86%. |
| Rashid et al. [29] | 2019 | DNA sequence encoding | Anomaly | KDDCup 99 and NSL-KDD | DR = 99.47%<br>FAR = 35.24%<br>Accuracy = 92.71% |
| Rashid [30] | 2020 | DNA sequence encoding | Misuse | UNSW-NB15 | DR = 90.91%<br>FAR = 24%<br>Accuracy = 89.05% |
| Dutt et al. [31] | 2020 | Immune System | Anomaly | KDD99 and UNSW-NB15 | TP = 97% based on real-time traffic and standard data sets. |
| Rashid et al. [32] | 2021 | DNA sequence encoding | Anomaly | KDD99 and UNSW-NB15 | DR = 99.58%<br>FAR = 35.53%<br>Accuracy= 92.74% |
| Rashid & Al-Hakeem [33] | 2022 | DNA sequence encoding | Hybrid | UNSW-NB15 | DR = 81.22%<br>FAR = 12.2%<br>Accuracy= 82.05% |

### 3.3 Evolutionary Techniques for IDS

An evolutionary computation technique is inspired by natural evolution. In the security domain, the most studied area was the IDS. Evolutionary computation has various characteristics, such as

generating readable outputs, easing representation, and producing lightweight solutions. These characteristics attract researchers to investigate these techniques on IDS. [34].

Genetic algorithm is one of the most common evolutionary techniques methods. A genetic algorithm was built initially for the computational biology field using computers to select and evaluate the processes. Crosbie and Spafford [35] merged the genetic algorithm with IDS. However, the main drawback of applying a genetic algorithm for IDS is that it may lead to high FAR results and time-consuming if choosing incorrect threshold values. Table 4 shows the reviews of some IDS using evolutionary techniques.

**Table 4- Reviews for some IDS based on evolutionary techniques**

| Author(s) | Year | Method(s) | Detection Methodology | Dataset | Performance |
|---|---|---|---|---|---|
| Li et al. [36] | 2011 | Ant Colony and Fuzzy C-means | - | KDDCup 99 | DR:<br>Dos = 95.34%<br>Probe = 90.03%<br>R2L = 13.82%<br>U2R = 34.18%<br>Normal = 99.41% |
| Cai & Yuan [37] | 2013 | Ant Colony | Anomaly | KDDCup 99 | Precision = 96.94%<br>Recall = 98.41% |
| Padmadas et al. [38] | 2013 | Genetic Algorithm | - | Collected data | R2L attack:<br>Accuracy = 90%. |
| Qiang et al. [39] | 2016 | Ant Colony | Anomaly | KDDCup 99 | DR:<br>DoS = 93.1%<br>Probe = 92.2%<br>R2L = 90.7%<br>U2R = 95.5% |
| Varma et al. [40] | 2016 | Ant Colony | - | UCI Cleveland | Accuracy is increased by 0.11%<br>Time is faster by 37.19% |
| Tabatabaefar et al. [41] | 2017 | Particle Swarm | Anomaly | KDDCup 99 | DR = 99.1%<br>FAR = 1.9% |

| | | | | | |
|---|---|---|---|---|---|
| | | Optimization | | | Accuracy = 99.58% |
| Punitha et al. [42] | 2019 | Genetic Algorithm | - | KDDCup 99 | Recall:<br>Normal = 98.8%<br>U2R = 86.6%<br>DoS = 93.8%<br>R2L = 91.9%<br>Prope = 89.8% |

3.4 Machine Learning for IDS

Several IDS were proposed based on machine learning techniques, either based on single learning techniques such as Bayesian Network and Fuzzy Logic or combining two or more learning techniques such as ensemble techniques [43].

Bayesian network is a graphical representation for variables set, and this algorithm can get results from probabilistic information. An efficient IDS can be proposed based on this algorithm [42]. Another machine learning technique is Fuzzy logic, a form of many-valued logic that deals with approximate this algorithm that have been applied in the security field since 1993 [44]. IDS has been proposed based on the Fuzzy method because of this method's ability to consider the features as fuzzy variables. However, the main disadvantage of applying fuzzy logic for IDS is the high resource consumption. Also, ensemble learning is another example of a machine learning technique, and this system has many classifiers. Each classifier can search separately and integrate all results, leading to better learning than a single classifier [45]. Examples of ensemble algorithms are bagging and boosting. Table 5 shows the reviews of some IDS using machine learning algorithms.

**Table 5- Reviews for some IDS based on machine learning methods**

| **Author(s)** | **Year** | **Method(s)** | **Detection Methodology** | **Dataset** | **Performance** |
|---|---|---|---|---|---|
| Altwaijry & Algarny [46] | 2012 | Naive Bayesian | Anomaly | KDDCup 99 | DR:<br>Dos = 99.36%<br>Probe = 57.17%<br>R2L = 0%<br>U2R = 0%<br>All attacks = |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 89.70% |
| Koc et al. [47] | 2012 | Hidden Naïve Bayes | - | KDDCup 99 | Accuracy = 93.27%<br>Error rate = 6.28% |
| Modi et al. [48] | 2012 | Bayesian Classifier and Snort | Hybrid | KDDCup 99 | Accuracy = 97.07%<br>Base rate = 77.06% |
| Li & Lin [49] | 2013 | Rough Classifiers | - | 1999 DARPA | FAR = 10.40%<br>DR:<br>DoS = 86.25%<br>Probe = 89.56%<br>R2L = 73.49%<br>U2R = 76.67% |
| Chapke & Deshmukh [50] | 2015 | Fuzzy Logic and C4.5 | - | KDDCup 99 | DR = 99.47%<br>FAR = 2.75% |
| Gaikwad & Thool [51] | 2015 | Bagging method | - | NSL-KDD | DR = 78.4%<br>FAR = 17.2%<br>Accuracy = 78.37% |
| Sreenath & Udhayan [52] | 2015 | Bagging method | Anomaly | NSL-KDD | Accuracy = 97.85% |
| Farnaaz & Jabbar [53] | 2016 | Random Forest | Anomaly | NSL-KDD | Best DR = 99.84%<br>Accuracy = 99.67% |
| Rodda & Erothi [54] | 2016 | Machine learning | - | NSL-KDD | DR:<br>DoS = 95.1%<br>Probe = 98.13%<br>R2L = 93.35%<br>U2R = 19.04% |
| Jabbar et al. [55] | 2017 | Ensemble classifier | Anomaly | Kyoto | DR = 92.38%<br>FAR = 0.14%<br>Accuracy = 90.51% |
| Mkuzangwe & Nelw Amondo [56] | 2017 | Fuzzy Logic | - | NSL-KDD | Accuracy = 93.24% |
| Belouch et al. [57] | 2018 | Machine | - | UNSW- | DR = 97.49% |

| | | | | | |
|---|---|---|---|---|---|
| | | learning | | NB15 | Accuracy = 93.53% |
| Idhammad et al. [58] | 2018 | Naive Bayes | Anomaly | CIDD-001 | FAR = 0.21%<br>Accuracy = 97.05% |
| Verma & Ranga [59] | 2018 | K-nearest neighbor | Anomaly | CIDD-001 | Accuracy with different number of neighbors = 95%, 96%, 94%, 95%, and 93%. |
| Halimaa & Sundarakantham [60] | 2019 | Machine Learning | - | NSL-KDD | Accuracy = 97.29%<br>Misclassification = 2.705% |
| Yihunie et al. [61] | 2019 | Machine Learning | Anomaly | NSL-KDD | Precision = 99.92%<br>Recall = 99.69%<br>F-score = 99.80% |
| Amouri et al. [62] | 2020 | Machine Learning | - | - | DR = 98% |

3.5 Pattern Recognition for IDS

Pattern recognition algorithms are used to provide a reasonable answer for all possible inputs and do matching for these inputs. A regular expression is an example of pattern matching algorithms that look for patterns in textual data and are available in many text editors [63]. Pattern recognition algorithms are divided based on label output type either the learning is supervised (Classification algorithms) or unsupervised (Clustering algorithms). The classification was applied in different applications dealing with huge data, such as plaintext classification, medical diagnosis, IDS, etc. Examples of classification techniques used for IDS are decision trees, support vector machines, and others. On the other hand, clustering is the process of dividing objects into two or more groups called clusters, and this method has been applied for IDS. An example of clustering algorithms are k-means and fuzzy c-means. Table 6 shows the reviews of some IDS using pattern recognition methods.

**Table 6- Reviews for some IDS based on pattern recognition method**

| **Author(s)** | **Year** | **Method(s)** | **Detection Methodology** | **Dataset** | **Performance** |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Ganapathy et al. [64] | 2012 | Fuzzy C-Means and Immune genetic algorithm | - | KDDCup 99 | Recall = 94.16%<br>Precision = 94.86%<br>FCM based on Immune genetic algorithm gave better FAR result than FCM only. |
| Karthick et al. [65] | 2012 | Hidden Markov Model | - | 1999 DARPA | Accuracy = 97.1%<br>FAR = 2.71% |
| Modil et al. [66] | 2012 | Bayesian Networks | Hybrid | KDDCup 99 | Base rate = 74.68%<br>TP = 96.57%<br>Accuracy = 97.07% |
| Mohammad & Sulaiman [67] | 2012 | SVM | Hybrid | Collected data | Accuracy = 99.60%<br>CPU run time = 15.44 seconds |
| Eslamnezhad & Varjani [68] | 2014 | MinMax K-means | Anomaly | NSL-KDD | DR = 81%<br>FP = 9% |
| Kim et al. [69] | 2014 | C4.5 Decision Tree | Hybrid | NSL-KDD | Detection time:<br>Training = 21.37 seconds<br>Testing = 10.13 seconds |
| Fossaceca et al. [70] | 2015 | Extreme Learning Machines | - | KDDCup 99 | DR:<br>DoS = 99.96%<br>Probe = 97.42%<br>R2L = 94.94%<br>U2R = 62.87% |
| Kao et al. [71] | 2015 | Pattern Matching | - | - | Performance = 86%<br>reduce the size by 20% |
| Chen et al. [72] | 2016 | Hidden Markov Model | Anomaly | Collected data | Accuracy = 86.2%<br>Precision = 93.2%<br>Recall = 84.1% |

| | | | | | |
|---|---|---|---|---|---|
| Yin et al. [73] | 2016 | SVM and context validation | Anomaly | KDDCup 99 | Training time = 522 seconds.<br>Recall = 98.40%<br>Accuracy = 94.16%<br>Precision = 94.79% |
| Ikram & Cherukuri [74] | 2017 | SVM and chi-square | - | NSL-KDD | Training time = 10 seconds<br>Testing time = 235 seconds<br>The highest accuracy = 98.1%<br>The best FAR = 1.9% |
| Wei et al. [75] | 2017 | Intra-class distance | - | KDDCup 99 | Training time = 92 seconds<br>DR = 98.75%<br>FAR = 16.88% |
| Yang et al. [76] | 2017 | Fuzzy interpolation | Misuse | NSL-KDD | DR:<br>DoS = 98.15%<br>Probe = 74.11%<br>R2L = 75.99%<br>U2R = 45.71%<br>Accuracy = 74.41% |
| Yuan et al. [77] | 2017 | C5.0 method and Naive Bayes algorithm | - | KDDCup 99 | DR:<br>DoS = 97.33%<br>Probe = 87.74%<br>R2L =12.71%<br>U2R = 51.43%<br>FAR = 6.44%<br>Accuracy = 93.32% |
| Idris et al. [78] | 2019 | SVM and Cat Swarm Optimization | Anomaly | NSL-KDD | Accuracy = 96.3%<br>Precision = 95.4%<br>Recall = 97.9% |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | FP = 0.02% |
| Liang et al. [79] | 2019 | SVM | - | NSL-KDD | Accuracy = 94.51% Time = 127.34 seconds |
| Liu et al. [80] | 2020 | SVM | Anomaly | UNM | DR = 92.63% FAR = 6.16% |

## 4. Conclusion

This paper introduced an overview of the concepts, detection methods and techniques for IDS. The IDS techniques literature has been discussed in detail, and these techniques have been categorized into ANN, bio-inspired computing, evolutionary technique, machine learning, and pattern recognition. Each technique has its advantages and disadvantages; therefore, the selection of approach must be cautious and consider the techniques superiority and limitations.

## Refrences

[1]. Euismod in pellentesque massa placerat. Morbi non arcu risus quis varius quam quisque.P. Adlakha and P. Subramanium, “Various approaches for detecting attacks in intrusion detection system”, International Journal of Computer Science and Mobile Computing vol. 2, no. 3, pp. 1-3, 2013.

[2]. N. Boudriga, Security of mobile communications, Boca Raton: CRC Press, 2010, p. 612.

[3]. C. Thomas, “Performance enhancement of intrusion detection systems using advances in sensor fusion. Supercomputer Education and Research Centre Indian Institute of Science”, Doctoral Thesis. 2009.

[4]. S. Theodorios, and K. Koutroumbas, Pattern Recognition, Academic press, 1999, p. 984.

[5]. J. Ryan, M. J. Lin, and R. Miikulainen, “Intrusion Detection with Neural Networks”, Advances in Neural Information Processing Systems vol. 10, pp. 943-949. 1998.

[6]. F. Haddadi, S. Khanchi, M. Shetabi, and V. Derhami, “Intrusion detection and attack classification using feed-forward neural network”, Second International Conference on Computer and Network Technology, Bangkok, Thailand, 2010.

[7]. J. Wang, and Y. Yu, “Research on hybrid neural network in intrusion detection system”, World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering vol. 7, no. 4, pp. 451-485. 2013.

[8]. W. Xing-Zhu, “Network intrusion prediction model based on RBF features classification”, International Journal of Security and Its Applications, vol. 10, no. 4, pp. 241-248, 2016.

[9]. L. Chun, G. Xiaoxian, Z. Jing, W. Wei, S. Hanji, and G. Peng, “Intrusion detection using end-to-end memory network”, Proceedings of the 2017 2nd International Conference on Communication and Information Systems, Wuhan, China, 2017.

[10]. J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, “Method of intrusion detection using deep neural network”, IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, South Korea, 2017.

[11]. A. Shenfield, D. Day, and A. Ayesh, “Intelligent intrusion detection systems using artificial neural networks”, ICT Express, vol. 4, no. 2, pp. 95–99, 2018.

[12]. P. Singh, P. J. Jaykumar, A. Pankaj, and R. Mitra, “Edge-Detect: Edge-Centric Network Intrusion Detection using Deep Neural Network”, IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021.

[13]. S. Goel, and S. F. Bush, “Biological models of security for virus propagation in computer networks”, Login, vol. 29, no. 6, 2004.

[14]. L. N. De Castro, and J. Timmis, Artificial immune systems: a new computational approach Publisher Springer-Verlag, 2002., p. 357.

[15]. Hofmeyr, S. A. & Forrest, S. A. Architecture for an artificial immune system. Evolutionary Computation 8(4): 443-473. 2000.

[16]. S. Forrest, L. Allen, A. S. Perelson, and R. Cherukuri, “Self-nonself discrimination in a computer”, Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202-212. 1994.

[17]. B. Yu, E. Byres, and C. Howey, “Monitoring Controller‟s DNA Sequence for System Security”, ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society, 2001.

[18]. G. Păun, “A quick introduction to membrane computing”, The Journal of Logic and Algebraic Programming, vo;. 79, no. 6, pp. 291-294, 2010.

[19]. T. Al-Ibaisi, A. Abu-Dalhoum, M. Al-Rawi, M. Alfonseca, and A. Ortega, “Network intrusion detection using genetic algorithm to find best DNA signature”, Wseas Transactions on Systems, vol. 7, no. 7, pp. 589-599, 2008.

[20]. Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, “Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid”, Power and Energy Society General Meeting, pp. 1-8. 2011.

[21]. A. S. Randrianasolo, and L. D. Pyeatt, “An artificial immune system based on Holland‟s classifier as network intrusion detection”, Machine Learning and Applications 2012 11th International Conference 1, pp. 504-507, 2012.

[22]. R. K. Idowu, A. Maroosi, R. C. Muniyandi, and Z. A. Othman, “An Application of Membrane Computing to Anomaly-based Intrusion Detection System”, Procedia Technology, vo;. 11, pp. 585-592, 2013.

[23]. S. M. Hameed, and O. F. Rashid,”Intrusion detection approach based on DNA signature”, Iraqi Journal of Science, vol. 55, no. 1, pp. 241-250, 2014.

[24]. F. Hosseinpour, P. V. Amoli, F. Farahnakian, J. Plosila, and T. Hämäläinen, “Artificial immune system based intrusion detection: innate immunity using an unsupervised learning approach”, International Journal of Digital Content Technology and its Applications, vol. 8, no, 5, pp. 1-12, 2014.

[25]. R. K. Idowu, R. C. Muniyandi, and Z. A. Othman, “Improving bee algorithm based feature selection in intrusion detection system using membrane computing”, Journal of Networks, vol. 9, no. 3, pp. 523-529, 2014.

[26]. O. F. Rashid, Z. A. Othman, and S. Zainudin, “A novel DNA sequence approach for network intrusion detection system based on cryptography encoding method”, International Journal on Advanced Science Engineering and Information Technology, vol. 7, no. 1, pp. 183-189, 2017.

[27]. F. Farahnakian, and J. Heikkonen, “A deep auto-encoder based approach for intrusion detection system”, International Conference on Advanced Communications Technology, Korea (South), 2018.

[28]. S. L. Suliman, M. S. Abd Shukor, M. Kassim, R. Mohamad, and S. Shahbudin, “Network Intrusion Detection System Using Artificial Immune System (AIS)”, 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 2018.

[29]. O. F. Rashid, Z. A., Othman, and S. Zainudin, “Four Char DNA Encoding for Anomaly Intrusion Detection System”, Proceedings of the 2019 5th International Conference on Computer and Technology Applications, 2019.

[30]. O. F. Rashid, “DNA Encoding for Misuse Intrusion Detection System based on UNSW-NB15 Data Set”, Iraqi Journal of Science, vol. 61, no. 12, pp. 3408-3416, 2020.

[31]. I. Dutt, S. Borah, and I. K. Maitra, “Immune System Based Intrusion Detection System (IS-IDS): A Proposed”, IEEE Access, vol. 8, pp. 34929–34941, 2020.

[32]. O. F. Rashid, Z. A. Othman, S. Zainudin, and N. A. Samsudin, “DNA Encoding and STR Extraction for Anomaly Intrusion Detection Systems”, IEEE Access, vol. 9, pp. 31892-31907, 2021.

[33]. O. F. Rashid, and M. S. Al-Hakeem, “Hybrid Intrusion Detection System based on DNA Encoding,Teiresias Algorithm and Clustering Method”, Webology, vol. 19, no. 1, 2022.

[34]. D. B. Fogel, “What is evolutionary computation?”, IEEE Spectrum, vol. 37, no. 2, pp. 26-32, 2000.

[35]. M. Crosbie, and E. H. Spafford, “Active defense of a computer system using autonomous agents”, Technical Report CSD-TR- 95-008, Purdue University, 1995.

[36]. W. S. Li, X. M. Bai, L. Z. Duan, and X. Zhang, “Intrusion detection based on ant colony algorithm of fuzzy clustering”, 2011 International Conference on Computer Science and Network Technology, Harbin, China, 2011.

[37]. C. Cai, and L. Yuan, “Intrusion detection system based on ant colony system”, Journal of Networks, vol. 8, no. 4, pp. 888-894, 2013.

[38]. M. Padmadas, N. Krishnan, J. Kanchana, and M. Karthikeyan, “Layered approach for intrusion detection systems based genetic algorithm”, Computational Intelligence and Computing Research 2013 IEEE International Conference, Enathi, India. 2013.

[39]. Y Qiang, H. Zhongyu, S. Shikai, and Z. Dawei, “Research of intrusion detection method based on ant colony clustering”, 4th International Conference on Machinery, Materials and Computing Technology, Hangzhou, China. 2016.

[40]. R. K. Varma, V. Kumari, and S. Kumar, “Feature selection using relative fuzzy entropy and ant colony optimization applied to real-time intrusion detection system”, Procedia Computer Science, vol. 85, pp. 503-510, 2016.

[41]. M. Tabatabaefar, M. Miriestahbanati, and J. Grégoire, “Network intrusion detection through artificial immune system”, Systems Conference (SysCon), 2017 Annual IEEE International, Montreal, QC, Canada, 2017.

[42]. A. Punitha, S. Vinodha, R. Karthika, and R. Deepika, “A Feature Reduction Intrusion Detection System using Genetic Algorithm”, 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 2019.

[43]. F. S. Tsai, “Network intrusion detection using association rules”, International Journal of Recent Trends in Engineering, vol. 2, no, 2, pp. 202-204, 2009.

[44]. H. Altwaijry, and S. Algarny, “Bayesian based intrusion detection system”, Journal of King Saud University-Computer and Information Sciences, vol. 24, no. 1, pp. 1-6, 2012.

[45]. H. H. Hosmer, “Security is fuzzy! Applying the Fuzzy Logic Paradigm to the Multipolicy Paradigm”, Proceedings on the 1992-1993 workshop on new security paradigms, pp. 175-184, 1993.

[46]. H. Zhao, “Intrusion Detection Ensemble Algorithm based on Bagging and Neighborhood Rough Set”, International Journal of Security and Its Applications, vol. 7, no. 5, pp. 193-204, 2013.

[47]. L. Koc, T. A. Mazzuchi, and S. Sarkan, “A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier”, Expert Systems with Applications, vol. 39, pp. 13492–13500, 2012.

[48]. C. N. Modil, D. R. Patell, A. V. Patd, and R. Muttukrishnan, “Bayesian classifier and snort based network intrusion detection system in cloud computing”, Computing Communication and Networking Technologies 2012 Third International Conference, Coimbatore, India, 2012.

[49]. S. Li, and F. Lin, “An efficient architecture for network intrusion detection based on ensemble rough classifiers”, The 8th International Conference on Computer Science & Education, Colombo, Sri Lanka, 2013.

[50]. P. P. Chapke, and R. R. Deshmukh, “Intrusion detection system using fuzzy logic and data mining technique”, Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology, Unnao, India, 2015.

[51]. D. P. Gaikwad, and R. C. Thool, “Intrusion detection system using bagging with partial decision treeBase classifier”, Procedia Computer Science, vol. 49, pp. 92-98, 2015.

[52]. M. Sreenath, J. Udhayan, “Intrusion detection system using bagging ensemble selection”, Engineering and Technology 2015 IEEE International Conference, Coimbatore, India, 2015.

[53]. N. Farnaaz, and M. A. Jabbar, “Random forest modeling for network intrusion detection system”, Procedia Computer Science, vol. 89, pp. 213-217, 2016.

[54]. S. Rodda, and U. S. R. Erothi, “Class imbalance problem in the Network Intrusion Detection Systems”, Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference, Chennai, India, 2016.

[55]. M. A. Jabbar, R. Aluvalu, and S. S. Reddy, “RFAODE: a novel ensemble intrusion detection system”, Procedia Computer Science, vol. 115, pp. 226–234, 2017.

[56]. N. N. P. Mkuzangwe, and F. V. Nelwamondo, “A Fuzzy Logic Based Network Intrusion Detection System for Predicting the TCP SYN Flooding Attack”, Intelligent information and database systems 9th Asian conference, Kanazawa, Japan, 2017.

[57]. M. Belouch, S. ElHadaj, and M. Idhammad, “Performance evaluation of intrusion detection based on machine learning using Apache Spark”, Procedia Computer Science, vol. 127, pp. 1-6, 2018.

[58]. M. Idhammad, K. Afdel, and M. Belouch, “Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques”, Procedia Computer Science, vol. 127, pp. 35-41, 2018.

[59]. A. Verma, and V. Ranga, “Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning”, Procedia Computer Science, vol. 125, pp. 709-716, 2018.

[60]. A. A. Halimaa, and K. Sundarakantham, “Machine Learning Based Intrusion Detection System”, 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019.

[61]. F. Yihunie, E. Abdelfattah, and A. Regmi, “Applying Machine Learning to Anomaly-Based Intrusion Detection Systems”, 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2019.

[62]. A. Amouri, Y. T. Alaparthy, and S. D. Morgera, “A Machine Learning Based Intrusion Detection System for Mobile Internet of Things”, Sensors, vol. 20, no. 2, 2020.

[63]. C. M. Bishop, Pattern recognition and machine learning, Springer, 2011, p. 738.

[64]. S. Ganapathy, K. Kulothungan, P. Yogesh, and A. Kannan, “A novel weighted fuzzy c–means clustering based on immune genetic algorithm for intrusion detection”, Procedia Engineering, vol. 38, pp. 1750-1757, 2012.

[65]. R. R. Karthick, V. P. Hattiwale, and B. Ravindran, “Adaptive network intrusion detection system using a hybrid approach”, Communication Systems and Networks 2012 Fourth International Conference, Bangalore, India, 2012.

[66]. C. N. Modil, D. R. Patell, A. V. Patd, and R. Muttukrishnan, “Bayesian classifier and snort based network intrusion detection system in cloud computing”, Computing Communication and Networking Technologies 2012 Third International Conference, Coimbatore, India, 2012.

[67]. M. N Mohammad, N. Sulaiman, and O. A. Muhsin, “A novel intrusion detection system by using intelligent data mining in weak environment”, Procedia Computer Science, vol. 3, pp. 1237–1242, 2012.

[68]. M. Eslamnezhad, and A. Y. Varjani, “Intrusion detection based on minmax k-means clustering”, 2014 7th International Symposium on Telecommunications, Tehran, Iran, 2014.

[69]. G. Kim, S., Lee, and S. Kim, “A novel hybrid intrusion detection method integrating anomaly detection with misuse detection”, Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, 2014.

[70]. J. M. Fossaceca, T. A. Mazzuchi, and S. Sarkani, “MARK-ELM: application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection”, Expert Systems with Applications, vol. 42, no. 8, pp. 4062-4080, 2015.

[71]. C. Kao, I. Liao, Y. Chang, C. Lin, N. Huang, R. Liu, and H. Hung, “A retargetable multiple string matching code generation for embedded network intrusion detection platforms”, Communication Software and Networks (ICCSN), 2015 IEEE International Conference, Chengdu, China, 2015.

[72]. C. Chen, D. Guan, Y. Huang, and Y. Ou, “Anomaly network intrusion detection using hidden Markova model”, International Journal of Innovative Computing, Information and Control, vol. 12, no. 2, pp. 569–580, 2016.

[73]. G. Yin, Y. Zhang, and Z. Zhao, “A novel computer network intrusion detection algorithm based on OSVM and context validation”, 2016 International Conference on Progress in Informatics and Computing (PIC), Shanghai, China, 2016.

[74]. S. T. Ikram, and A. K. Cherukuri, “Intrusion detection model using fusion of chi-square feature selection and multi class SVM”, Journal of King Saud University – Computer and Information Sciences, vol. 29, pp. 462–472, 2017.

[75]. L. Wei, C. Ya-ping, Y. Zhong-Ming, and Z. Bin, “A clustering algorithm oriented to intrusion detection”, 2017 IEEE International Conference on Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2017.

[76]. L. Yang, J. Li, G. Fehringer, P. Barraclough, G. Sexton, and Y. Cao, “Intrusion detection system by fuzzy interpolation”, 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Naples, Italy, 2017.

[77]. Y. Yuan, L. Huo, and D. Hogrefe, “Two layers multi-class detection method for network intrusion detection system”, 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 2017.

[78]. S. Idris, O. Oyefolahan Ishaq, and N. Ndunagu Juliana, “Intrusion Detection System Based on Support Vector Machine Optimized with Cat Swarm Optimization Algorithm”, 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf), 2019.

[79]. D. Liang, Q. Liu, B. Zhao, Z. Zhu, and D. Liu, “A Clustering-SVM Ensemble Method for Intrusion Detection System”, 2019 8th International Symposium on Next Generation Electronics (ISNE), 2019.

[80]. W. Liu, L. Ci, and L. Liu, “A New Method of Fuzzy Support Vector Machine Algorithm for Intrusion Detection”, Applied Sciences, 2020.