Intrusion-Detection System Based on Hybrid Models: Review Paper

Mohammed falih badran¹, Nan Md. Sahar*¹,², Suhaila Sari¹, N. S. A. M. Taujuddin¹

²Microelectronics & Nanotechnology - Shamsuddin Research Centre (MiNT-SRC), ¹Faculty of Electrical and Electronic Engineering (FKEE) ,Universiti Tun Hussein Onn Malaysia, Parit Raja, Johor

*nan@uthm.edu.my

Abstract. The Intrusion-detection systems (IDS) is currently one of the most important security tools. However, an IDS-based hybrid model offers better results than crime detection using the same algorithm. However, hybrid models based on conventional algorithms still face different problems. The objective of this study was to provide information on the most important assumptions and limitations of close hybrid analysis based on criminal analysis and to analyze the limitations of the new machine learning algorithm (FLN) to obtain IDS-based advice.

Keywords: Extreme Learning Machine, Fast Learning Network, Intrusion Detection System, Optimization

1. Introduction

In the past few years, technology has been influenced by many applications today, including business, shopping and the media. [1]. One of the major problems is that these systems are constantly exposed to many online threats that threaten access and therefore demand protection against infringement. In 2015, Admiral Michael Rogers, head of the US National Security Agency, warned the House Intelligence Committee of a major security attack in the United States over the next decade. In his words, “It’s only a matter of the ‘when,’ not ‘if,’ that we are going to see something dramatic.”

Many government-run programmers attack the mechanically controlled framework of nuclear energy, energy grid, and transportation. Along with the framework of transportation and the aviation authority that oversees, transportation systems, and air-traffic control, the chief executive of the US National Security Agency has suggested that the United States may be victim in these attacks, given its own assessment [2].
In addition, the Intrusion detection system (IDS) is one of the most amazing programs or devices of software and hardware [3] that is used to check the configuration of computers to find them regularly or irregularly [4] [5]. The IDS system tests system interception indicators that may appear in unusual framework ways or may violate system security strategies. In addition, there are the usual barriers to IDS [6], [7], for example, advanced counterfeit alerts, lack of continuous correction to change retaliation, and the allocation of highly balanced information. In addition, artificial intelligence of machine learning (ML) combinations can improve IDS delivery and performance [8], [9] as ML accounts can guarantee maximum performance. It provides some commitment based on ML models: It first tests the most advanced ML-based ID models, as well as some current extremes that can drill into ML-dependent models. Various applications of remote sensing and transport of information systems, such as crisis management and welfare, demonstrate the risk of various digital threats, disruptions, and attacks resulting from the transparency of these systems. The data information communication infrastructure framework has exceptionally improved the lives of current society. Be that as it may, this foundation is constantly under the dangers of interruption and misuse. So as to evacuate such dangers the exploration and industry network have thought of various risk recognition and technologies. One of such innovation is Intrusion Detection Systems (IDS).

2. Overview of Intrusion Detection System

In today's world, mechanical and technological advanced methods have made access easier than ever. [10]. A lot of data (individual, military, and government, business and commercial) is facilitated in conducting the framework around the world. One of the most important research challenges in the well-being of these systems is the detection of defects, the purpose of which is to identify the strange behaviors of the system in order to ensure the safe and strong activities and parts of the system. Further closure is characterized by the development of a multifunctional framework and a compensation system. The security of the system's framework is largely due to the scientific features that can be effectively accessed all over the web, attracting an extraordinary amount of research enthusiasm. Audiences are increasingly relying on technology as individuals rely on personal computer frameworks for their data and everyday entertainment.[11].

In addition, IDS represents to the amazing security Agency and tool, which monitors frame drills and activities for any malicious performance or system security breaches. In addition, the IDS plays several capabilities [12], for example, monitoring and evaluating the client's framework performance, testing the basic framework, and smoothing the recording. Generally, IDS strategies that have been isolated due to abuse or misuse are used to identify misuse through a site framework, and these procedures are described below. The table defines the IDS [9], [13] authentication, which is the main difference between IDS modes.
Table.1 comparison between Anomaly and signature detection

| Aspects | Anomaly Detection | Signature |
|---------|-------------------|-----------|
| Characteristics | Utilizations the deviation from ordinary use | Examples to recognize and identify intrusions using know attack signatures. |
| Drawbacks | Must investigate the consecutive and sequential interrelation between exchanges, False positives. | attacks must be coded manually and physically; can't identify new attacks |

In addition, proposed IDS models based on, for example, improving computation leads to better results in appropriate and single algorithm models or strategy-based models, for example, [14], [15], [16] [17] - [20]. However, most of these hybrid models have limitations due to the fact that most of these models are added to the old algorithm account, and are still physically separate from the proposed model structure.

3. Overview of IDS based on Machine learning

Conventional and traditional systems such as firewalls, encryption, and access systems are reliably protected against advanced types of attacks and malware [12]. Resultantly IDS was formed as an important part of the security framework used before the attacks, even before the occurrence [21] [22]. There are definitely some things to keep in mind when creating IDS systems, including classifying information, verifying interference, providing advanced information, disclosing and responding to it. The most important to these issues is recognition of intrusion.

In addition, ML was not acceptable until the time of the request and the accuracy of the time of protesting these requests were acceptable [23]. Fortunately, there is a shortage of computational knowledge methods to demonstrate compatibility with internal failure, which are sincerely sympathetic due to high computational and fast information. Most ML-based frameworks are not defensible against high levels of false positive and negative caution. In addition, they are not able to permanently modify their attack patterns [24]. In order to defeat most of these ML limitations, several optimization techniques and enhanced systems have been modified. These methods include the genetic algorithm (GA), the bee algorithm, and the particle swarm optimization (PSO). This relies on a wide range of durable identifiers that rely on reciprocal and hybrid models. The Interference Detection Framework monitors events in the computer or system mode and warns the human operator of potential abuse of standard security procedures. Identity innovation can be configured as a host identifier or web-based identifier depending on the transfer area. Depending on the strategy used to analyze the
collected data, IDS can be classified into two broad categories as Misuse based detection and anomaly based detection. To date, various and varied methods of design and artificial intelligence have been used to create the (IDPS), but no complex audits have been reported for exhibition. And the consequences of such a method do not determine a remote situation.

4. Main Structure of Proposed Model

This section is about explaining a proposed model that includes basic firewall accounts and fast learning network accounts. In addition, this section has standards for the new model (FA-FLN) according to IDS.

4.1 Overview of Fast Learning Network

The FLN consists of a cohesive three-layer feed forward neural network (FFNN) parallel to a three-layered FFNN that includes information, overlays, and output layers [25]. Figure 1 shows the structure of the FLN. Acceptance of many of the desired discrete N samples in the of the i th sample, and \( y_i = [y_{i1}, y_{i2}, \ldots, y_{in}]^T \in \mathbb{R}^l \) being the associated I-dimension output vector. Let's talk about the M that represents nodes in the hidden layer and this can be explained as the amount of neurons in the mixed layer can be solved using different solutions. For example, by determining the amount of hidden neurons in the middle of the information size and output layers, it can be used very appropriately [26]. The active function of the hidden nodes is represented by \( y(.) \) [27]. FLN can be modeled mathematically using the provided vectors and matrices as in the equations:

\[
y_j = f(\sum_{k=1}^{m} w_{jk}^i x_j + b_k) \quad \ldots \quad (1)
\]

Where \( j = 1, 2, \ldots , N \), \( w_{oj} = [w_{1oj}, w_{2oj}, \ldots , w_{noj}] \) represent the vector that connects with the \( j \) th input and output nodes, \( w_{ik} = [w_{1ik}, w_{2ik}, \ldots , w_{nik}] \) presents the weight vector that connects the \( k \) th input and hidden nodes, \( w_{ojh} = [w_{1ojh}, w_{2ojh}, \ldots , w_{noj}] \) represent the weight vector that connects the \( k \) th output and hidden nodes, and \( b_k \) is the biases of the \( k \) th hidden nodes. A more solid representation is provided as follows:

\[
Y = w_{oi}^o x + w_{oh}^o G = [w_{oi}^o w_{oh}^o] X_G = W X_G \quad \ldots \quad (2)
\]

Where

\[
G (W_{1}^{in}, \ldots , W_{m}^{in}, W_{1}, \ldots , b_{m}, \ldots , X_{N}) \quad \ldots \quad (3)
\]

\[
= \begin{bmatrix}
g(W_{1}^{in} x_{1} + b_{1}) & \cdots & g(W_{1}^{in} x_{N} + b_{1}) \\
\vdots & \ddots & \vdots \\
g(W_{m}^{in} x_{1} + b_{m}) & \cdots & g(W_{m}^{in} x_{N} + b_{m})
\end{bmatrix}_{m \times N}
\]
\[ W = [W^{oi} W^{oh}]_{1 \times (n + m)} \]  \hfill (4)

The matrix \( W = [W^{oi} W^{oh}] \) represent the output weights while \( G \) represents the output matrix of the FLNs’ hidden layer. A Moore-Penrose generalized inverse is used to resolve the model [28]. The minimum norm least-squares solution of the linear system could be expressed thus:

\[
\tilde{\omega} = \left( Y \right) \left[ X_{G} \right]^{+}
\]  \hfill (5)

\[
w^{oi} = \tilde{\omega}(1:1, 1:n) \\
w^{oh} = \tilde{\omega}(1:1, n + 1:n + m)
\]  \hfill (6)

Figure 1 shows the algorithm that clarified the FLN learning process. This algorithm is started by arbitrarily initializing the weights between the information input layer and the closed layer before proceeding with the finding of the frame \( G \) according to the hidden matrix network. This grid is a representation of the performance structure of hidden layers. Next, the Moore-Penrose conditions are used to find out the information performance framework \( (w^{oi} \text{ and } w^{oh}) \).

Also, according to Figure 1, which shows the FLN calculation of algorithm steps, which starts with random insertion of key parameters, this means that the algorithm may not have the best accuracy [17] [19] [22]. Many development algorithms were made. For example, the genetic algorithm (GA), Particle Swarm Optimization (PSO) and harmonic search optimization (HSO) [14] to reduce the fast parameters of a hybrid model. However, an effective simple algorithm, even if it has not yet encountered limited restrictions, for example, is not an ideal feature for parameters and algorithm structures that allow the most recent free parameters of algorithms.
5. Overview of Intrusion Detection System Based on Hybrid Models

There are many ML structures depending on the IDS. It has been suggested by [29] that IDS research can be organized into two main areas: identification of anomalies and data reduction. This strategy revolves primarily around learning techniques so as to select the ID to identify the disorder. The FLN has already been introduced for higher display on ELM and SVM where it has speed, ease of use and accuracy. It has been proven that ML-based IDs are able to use FLN to maximize their experience with more basic data, as opposed to the vast majority of data currently available in many tests. This can be done primarily due to the proximity to FLN's proposed direct measurement capacity without increasing the preparation time.

[30] Provide an overview of the network dependent on IDS and describe its effects as ANN and hybrid ANN. In simple terms, he studied for restlessness using BPNN, SVM, SA, and SOM. The hybridization approach focuses on the use of multiple methods. [31] Leads to revision of potential identification strategies. The NN SVM study guarantees and recommends that ELMs support their use for IDS, faster learning speed, higher visualization ability, and working with indirect components and capabilities. Although many studies have suggested that ELM is useful in overcoming most of these problems [32], precise details of previous tests on ELM with IDS have not been provided. Furthermore, the most efficient way to use ELM on ID was not discussed. In addition, they suggest an opportunity to overcome individual algorithm difficulties by combining different learning approaches.

[33] an SVM-based filtering algorithm ID is proposed to define different role selection tasks in the NSL-KDD dataset. The overall accuracy of the proposed algorithm was implemented correctly using only 3 inputs and 99\% 36 features, while all 41 features from the NSL-KDD group achieved implementation of accuracy. After that, the test set was performed with a density of 0.77. To the extent that poor estimation skills did not exist, this method does not significantly detect mysterious and anonymous system attacks. [34] Got the best results with a primary ELM. Choosing a department is an important step toward achieving a fair and meaningful learning but the included ELM piece is little more than an information test and requires a lot of memory. A large dataset cannot be deployed simultaneously due to memory problems, and in the dataset that performs a whole algorithm needs one way to combine multiple classes or bits to get results.

[15] A review of the refinement of the multi-tier learning option to more accurately define isolation as opposed to individual classifications. This classification of classifiers is convinced that past experiments have shown the ability of most classifiers to identify explicit chapters on the issue of multilevel learning. The introduction of a novel Multiple Adaptive Reduced Kernel ELM (MARK-ELM)-based IDS made MARK-ELM suitable for the processing of multi-class network IDS. While some tactics have been helpful in some attack classes, because they rely on KDD 99 and their performance is very poor. This proposed approach led to the rapid and logical identification of the positives that system face in dealing
with them. [35] Use large amounts of information, low detection rates, and false as common IDS problems. Use the continuous online ELM to configure IDS-based compatibility to manage traffic research. The proposed technology was evaluated in a standard data set from Kyoto University College. The recently used item was removed from the KDD info repository data. This algorithm has not been verified in many databases, such as KDD, and further verification is required.

Heuristic is a method of learning, descending, or critical thinking that uses an efficient method that is not optimal. [16] He presented an unusual strategy based on GA and SVM. GA and SVM to improve the management process and classification performance was used by them, the proposed system was examined in the KDDCUP '99 group. As shown in the SVM reservation, it collects parallel as general information or attack. The KDD '99 data repository was also included. Table 2 shows some of the tasks related to the ID [36] has proposed a strategy to define KNN intervention based on ant colony optimization and improvement (ACO). The algorithm with ACO was pre-configured using the KDD-Cup '99 data set, while exposure to KNN-ACO, BP, and SVM depended on normal execution parameters. The study reported an overall accuracy of 94.17% and an overall FAR of 5.82% for the proposed algorithm. However, this account was created with only 26167 examples and has a medium volume of information.

Table 2 Related IDS works based on hybrid models

| Authors | Algorithm | Model Type | Single | Hybrid | Limitations |
|---------|-----------|------------|--------|--------|-------------|
| [22]    | PSO-Kernel FLN | Anomaly | –      | ✓      | The side effects of the proposed model did not show the accuracy of each class, the main accuracy is not as accurate as the main imbalance of the information index. |
| [14]    | PSO-FLN | Anomaly | –      | ✓      | - Arbitrarily select 10% of all data structure. |
| [37]    | PSO-SVM | Anomaly | –      | ✓      | - The data is divided into two for preparation and testing which does not depend so much on related work. |

The model raises the alert level.
- The model evaluates KDD99 based on each constraint.

- High Speed Warning
- The model is even not suitable during the auditions
- The faulty system cannot be correctly identified.

- SVM
  - Signature
  - ELM lower computational requirements than SVMs,
  - ELMs have shorter training time requirements than SVMs,
  - ELMs work directly on multi-class classification problems.

- Bees algorithm (BA)+ SVM
  - Anomaly
  - The benefits calculated using ELM are not the same as in design.
  - Another problem with shortening the rest of the product is its slow rate cost.

- BP + DBSCA N algorithm
  - Anomaly
  - On a good model, all actions are difficult because the vulnerable system can detect known attacks.

- GA+ Decision Tree algorithm
  - Anomaly
  - With the freedom, Bayes needs a lot of information to work. As such, an assessment of potential growth is risky.

- Naïve Bayes Decision Tree
  - Anomaly
  - This work evaluated based on KDD99, and we mentioned already the problems with this data set.
This work was reviewed on the basis of KDD99 and we consider it relevant in this dataset.

Table 2 shows that the hybrid models are in contrast the best accuracy and individual dependence model as reported in the previous section. In addition, specific IDSs produce better results than signatures of IDs. Then, the IDS dataset speaks to an important limitation; and for models most of the hybrid between machine learning and optimization algorithm reduced the impact of randomness when selecting the main parameter values. The importance of the strategies and procedures and their presentation and impediments are moreover broke down right now, the restrictions are tended to as difficulties to acquire a lot of necessities for IDPS in setting up a communitarian based remote IDPS compositional structure.

6. Conclusion

The intrusion detection works well together and is the only mathematical model of the single algorithm. Most likely, most of these interconnected and hybrid models face numerous obstacles and limitations that represent the impetus and motivate to propose another hybrid model. Similarly, according to the previously introduced analysis-related work, it introduced another hybrid model called FA-FLN, which includes firefly algorithm and a fast learning system, which can handle a large majority of the limitations of the former frameworks. Breaking the boundaries of the previous structure. The main purpose of this article is to review and manage current Intrusion Detection and Prevention Systems (IDPS), related to traditional fraudulent mathematical approaches with the help of several experts. In addition, it is worth noting that currently, strategies, procedures, exhibitions and barriers have been eliminated and many of the IDPS requirements have been met in the IDPS formula based on Co-WIDPS.

Reference

[1] H. A. S. Ahmed, M. H. Ali, L. M. Kadhum, M. Fadli, B. Zolkipli, and Y. A. Alsaieria, “A Review of Challenges and Security Risks of Cloud Computing,” *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 1, pp. 87–91, 2016.

[2] J. M. Fossaceca, “Application of a Novel Multiple Kernel Learning Framework for Improving the Robustness of Network Intrusion Detection,” no. December 1992, 2015.
[3] M. H. Ali, M. F. Zolkipli, M. M. Jaber, and M. A. Mohammed, “Intrusion detection system based on machine learning in cloud computing,” *J. Eng. Appl. Sci.*, vol. 12, no. 16, pp. 4241–4245, 2017.

[4] E. Vasilomanolakis, S. Karuppayah, M. A. X. M. Uhlh, and M. Fischer, “55 Taxonomy and Survey of Collaborative Intrusion Detection,” vol. 47, no. 4, pp. 1–33, 2015.

[5] M. H. Ali, M. Fadlizolkipi, A. Firdaus, and N. Z. Khidzir, “A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System,” *2018 IEEE Student Conf. Res. Dev.*, pp. 1–4, 2019.

[6] S. A. R. Shah and B. Issac, “Performance comparison of intrusion detection systems and application of machine learning to Snort system,” *Futur. Gener. Comput. Syst.*, vol. 80, pp. 157–170, 2018.

[7] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, “Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,” *Expert Syst. Appl.*, vol. 67, pp. 296–303, 2017.

[8] M. H. Ali, K. Moorthy, M. Morad, and M. A. Mohammed, “Propose a New Machine Learning Algorithm based on Cancer Diagnosis,” no. October 2018, 2019.

[9] M. H. Ali and M. F. Zolkipli, “Review on Hybrid Extreme Learning Machine and Genetic Algorithm To Work As Intrusion Detection System in Cloud Computing,” vol. 11, no. 1, pp. 460–464, 2016.

[10] M. H. Ali, “TOWARDS A EXCEPTIONAL DISTRIBUTED DATABASE MODEL FOR MULTI DBMS.” pp. 553–560, 2014.

[11] Bhavya Daya, “Network security: History, importance, and future,” *Univ. Florida Dep. Electr.*, p. 13, 2013.

[12] T. Kaur, V. Malhotra, and D. Singh, “Comparison of network security tools-Firewall, Intrusion Detection System and Honeypot,” *Int. J. Enhanc. Res. Sci. Technol. Eng.*, vol. 3, no. 2, pp. 200–204, 2014.

[13] U. Kumar, “A Survey on Intrusion Detection Systems for Cloud Computing Environment,” vol. 109, no. 1, pp. 6–15, 2015.

[14] M. H. Ali, B. A. D. AL Mohammed, M. A. B. Ismail, and M. F. Zolkipli, “A new intrusion detection system based on Fast Learning Network and Particle swarm optimization,” *IEEE Access*, vol. XX, no. c, pp. 1–1, 2018.

[15] J. M. Fossaceca, T. A. Mazzuchi, and S. Sarkani, “Expert Systems with Applications MARK-ELM : Application of a novel Multiple Kernel Learning framework for improving the robustness of Network Intrusion Detection,” *Expert Syst. Appl.*, vol. 42, no. 8, pp. 4062–4080, 2015.

[16] B. M. A. R. M. Chizari and A. M. M. Eslami, “A hybrid method consisting of GA and SVM for intrusion detection system,” *Neural Comput. Appl.*, vol. 27, no. 6, pp. 1669–1676, 2016.

[17] M. H. Ali, “Intrusion Detection System Framework Based on Machine Learning for Cloud Computing,” no. September 2017, 2016.

[18] M. H. Ali, M. F. Zolkipli, M. A. Mohammed, and M. M. Jaber, “Enhance of extreme learning machine-genetic algorithm hybrid based on intrusion detection system,” *J. Eng. Appl. Sci.*, vol. 12, no. 16, pp. 4180–4185, 2017.
[19] M. H. Ali and M. Mohammed, “Optimize Machine Learning Based Intrusion Detection for Cloud Computing: Review Paper,” no. October, 2016.

[20] M. H. Ali and M. A. Mohammed, “An Improved Fast Learning Network with Harmony Search based on Intrusion-Detection System,” J. Comput. Theor. Nanosci., vol. 16, pp. 2166–2171, 2019.

[21] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion Detection Techniques in Cloud Environment: A Survey,” J. Netw. Comput. Appl., vol. 77, no. October 2016, pp. 18–47, 2016.

[22] M. H. Ali and M. F. Zolkipli, “Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System,” no. January, 2019.

[23] M. Zamani and M. Movahedi, “Machine Learning Techniques for Intrusion Detection,” pp. 1–11, 2013.

[24] X. W. Udaya Sampath K. Perera Miriya Thanthrige, Jagath Samarabandu, “Machine Learning Techniques for Intrusion Detection,” IEEE Can. Conf. Electr. Comput. Eng., pp. 1–10, 2016.

[25] G. Li, P. Niu, X. Duan, and X. Zhang, “Fast learning network: A novel artificial neural network with a fast learning speed,” Neural Comput. Appl., vol. 24, no. 7–8, pp. 1683–1695, 2014.

[26] Jeff Heaton, Introduction to Neural Networks with Java, vol. 99. 2008.

[27] M. F. Z. Mohammed Hasan Ali, “Intrusion-Detection System Based on Fast Learning Network in Cloud Computing,” no. September, 2018.

[28] N.-Y. Liang, G.-B. Huang, P. Saratchandran, and N. Sundararajan, “A Fast and Accurate Online Sequential Learning Algorithm for Feedforward Networks,” IEEE Trans. Neural Networks, vol. 17, no. 6, pp. 1411–1423, 2006.

[29] J. Xiang, M. Westerlund, D. Sovilj, and G. Pulkkis, “Using Extreme Learning Machine for Intrusion Detection in a Big Data Environment,” AISec’14, pp. 73–82, 2014.

[30] B. Shah and B. H. Trivedi, “Artificial Neural Network based Intrusion Detection System: A Survey,” vol. 39, no. 6, pp. 13–18, 2012.

[31] V. Jaiganesh, S. Mangayarkarasi, and P. Sumathi, “Intrusion Detection Systems: A Survey and Analysis of Classification Techniques,” vol. 2, no. 4, pp. 1629–1635, 2013.

[32] A. Patel, U. Universities, M. Taghavi, and K. Bakhtiyari, “An Intrusion Detection And Prevention System In Cloud Computing : A AN INTRUSION DETECTION AND PREVENTION SYSTEM IN CLOUD COMPUTING : A SYSTEMATIC REVIEW,” no. December 2017, 2012.

[33] M. S. Pervez and D. M. Farid, “Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs,” Ski. 2014 - 8th Int. Conf. Software, Knowledge, Inf. Manag. Appl., 2014.

[34] V. Jaiganesh and P. Sumathi, “Kernelized Extreme Learning Machine with Levenberg-Marquardt Learning Approach towards Intrusion Detection,” Int. J. Comput. Appl., vol. 54, no. 14, pp. 38–44, 2012.

[35] R. Singh, H. Kumar, and R. K. Singla, “An intrusion detection system using network traffic profiling and online sequential extreme learning machine,” Expert Syst. Appl., vol. 42, no. 22, pp. 8609–8624, 2015.
S. Vishwakarma, “An Intrusion Detection System using KNN-ACO Algorithm,” vol. 171, no. 10, pp. 18–23, 2017.

H. Saxena MTech Scholar and V. Richaariya, “Intrusion Detection in KDD99 Dataset using SVM-PSO and Feature Reduction with Information Gain,” Int. J. Comput. Appl., vol. 98, no. 6, pp. 975–8887, 2014.

O. Alomari and Z. A. Othman, “Bees Algorithm for feature selection in Network Anomaly detection β-Hill climbing for optimization problems View project Feature selection on high-dimensional data View project,” Artic. J. Appl. Sci. Res., vol. 8, no. 3, pp. 1748–1756, 2012.

R. Shivhare, S. Chaturvedi, and S. M. Tech, “A Novel and Hybrid Technique for Efficient Intrusion Classification,” vol. 3, no. 11, pp. 9124–9127, 2014.

B. Senthilnayaki, K. Venkatalakshmi, and A. Kannan, “An intelligent intrusion detection system using genetic based feature selection and Modified J48 decision tree classifier,” 2013 5th Int. Conf. Adv. Comput. ICoAC 2013, pp. 1–7, 2014.

D. H. Deshmukh, T. Ghorpade, and P. Padiya, “Improving classification using preprocessing and machine learning algorithms on NSL-KDD dataset,” Proc. - 2015 Int. Conf. Commun. Inf. Comput. Technol. ICCICT 2015, 2015.

G.-B. Huang, “Extreme learning machines for intrusion detection,” 2012 Int. Jt. Conf. Neural Networks, pp. 1–8, 2012.