Computers, Materials & Continua
DOI:10.32604/cmc.2020.013121
Article
Tech Science Press

Enhance Intrusion Detection in Computer Networks Based on Deep Extreme Learning Machine

Muhammad Adnan Khan[1,*], Abdur Rehman[2], Khalid Masood Khan[1], Mohammed A. Al Ghamdi[3] and Sultan H. Almotiri[3]

[1]Department of Computer Science, Lahore Garrison University, Lahore, 54792, Pakistan
[2]School of Computer Science, NCBA&E, Lahore, 54000, Pakistan
[3]Computer Science Department, Umm Al-Qura University, Makkah City, 715, Saudi Arabia
[*]Corresponding Author: Muhammad Adnan Khan. Email: madnankhan@lgu.edu.pk
Received: 27 July 2020; Accepted: 14 August 2020

Abstract: Networks provide a significant function in everyday life, and cybersecurity therefore developed a critical field of study. The Intrusion detection system (IDS) becoming an essential information protection strategy that tracks the situation of the software and hardware operating on the network. Notwithstanding advancements of growth, current intrusion detection systems also experience difficulties in enhancing detection precision, growing false alarm levels and identifying suspicious activities. In order to address above mentioned issues, several researchers concentrated on designing intrusion detection systems that rely on machine learning approaches. Machine learning models will accurately identify the underlying variations among regular information and irregular information with incredible efficiency. Artificial intelligence, particularly machine learning methods can be used to develop an intelligent intrusion detection framework. There in this article in order to achieve this objective, we propose an intrusion detection system focused on a Deep extreme learning machine (DELM) which first establishes the assessment of safety features that lead to their prominence and then constructs an adaptive intrusion detection system focusing on the important features. In the moment, we researched the viability of our suggested DELM-based intrusion detection system by conducting dataset assessments and evaluating the performance factors to validate the system reliability. The experimental results illustrate that the suggested framework outclasses traditional algorithms. In fact, the suggested framework is not only of interest to scientific research but also of functional importance.

Keywords: Intrusion detection system; DELM; network security; machine learning

1 Introduction

Networks are profoundly shaping daily life and making cybersecurity a significant study area. Cyber protection strategies comprise primarily virus protection applications, encryption, and Intrusion detection systems (IDS). Such strategies monitor networks from possible threats. Respectively, the IDS is a form of identification device that performs a crucial task in protecting network security by tracking the status of software and hardware operating on the network [1]. Cyber vulnerabilities associated with Denial of service (DoS) threats [2], Malware program [3], perhaps an unacceptable strategy resulting in irrecoverable destruction of the network and economic disasters. Statistics indicate that a malicious attack in May 2017 culminated in a huge $8 billion damage to a number of businesses, including finance, healthcare, infrastructure and academic institutions [4].

The network security infrastructure usually consists of a network defense mechanism and a data security program [5]. Although various systems, particularly security software and encryption, are designed to handle malware threats on the Network, the intrusion detection system is often expected to survive security threats on the network connection [6]. The purpose of an intrusion detection system is also to register, control, and identify unauthorized computer behaviors such as unlawful entry, modification, or interruption [7].

The very first framework for tracking intrusions was introduced in 1980. By then, several popular IDS applications have appeared. Nonetheless, several intrusion detection systems also endure from a strong false alarm rate, creating several warnings for lower non-threatening scenarios that increase the pressure on protection investigators and that trigger severe harmful threats to be missed. As a consequence, several experts have concentrated on improving intrusion detection systems with better detection levels and lower false alarm levels. One more issue with current intrusion detection systems is also that they lack the power to track unauthorized threats. Since network conditions are evolving rapidly, threat types and new threats are developing perpetually. It is therefore important to establish intrusion detection systems capable of detecting novel threats.

To order to resolve the aforementioned complications, scholars have started to work on designing intrusion detection systems employing machine learning approaches. Machine learning is a methodology of artificial intelligence that can continually learn valuable knowledge from large databases. Machine learning-based intrusion detection systems can reach a respectable degree of identification once adequate training information is accessible and machine learning frameworks are adequately generalizable to identify threat varieties and new threats. In comparison, machine-based intrusion detection systems do not depend extensively on domain experts; thus, they are simple to develop and build. Deep learning is a machine learning division which can produce excellent results. Similar to conventional machine learning approaches, deep learning strategies are ideally adapted when working with large dataset. In fact, deep learning approaches can dynamically acquire attribute interpretations through raw information and test outcomes; they run on an end-to-end basis and are realistic. The deep framework, which includes many hidden layers, is a fascinating aspect of deep learning. At the other side, conventional machine learning algorithms, including the support vector machine and the nearest neighbor, do not include any or even one hidden layer. Consequently, such typical types of machine learning are often considered shallow ones.

The objective for such analysis is to identify and outline the advanced deep extreme learning machine-based intrusion detection framework developed to be, to overview the important principles for applying machine learning to protection domain difficulties, and to examine existing issues and opportunities improvements. In this review, we chose relevant published papers between 2015 and 2019, that illustrate recent development. A few prior studies have listed work activities utilizing their advanced machine learning techniques [8–9].

To construct predictive security algorithms to analyze different developments in cyber-attacks and eventually anticipate the threats that can be used to build an insightful intrusion detection system that leverages information security information. The development of artificial intelligence solutions that can efficiently develop from a protection framework will also play a significant role in this process [10]. Security breaches are thus reduced in this work and this study incorporates an effective data-focused intrusion detection system in the area of network security. In this paper, we proposed a deep extreme learning machine-based intrusion detection system, which alleviates the above described issues. The advanced intrusion detection system, as traditional methods utilize a signature-based technique to identify specific configurations, is needed to address the underpinning problem. Nonetheless, candidate of the new technology termed as Deep extreme learning machine (DELM) can be used to analyze network traffic to identify intruders and threat trends. Machine Learning requires programs for training, understanding and acting without human involvement. The fundamental aim of machine learning is to construct an efficient method to collect data from inputs and simulate and modify outcomes through statistical observation. Machine learning can interpret a large quantity of information and render evidence-based judgments.

In our system, we formerly suggested the grouping of security factors in view of their importance in the paradigm. Consequently, we build an intrusion detection system built on the Deep Extreme Learning program security architecture centered on the listed key features. Once the system has been established leveraging training security understanding, the findings of the evaluation are used to validate the structure. The whole approach not just to succeeds in predicting reliability for unpredictable data sets by removing uncertainty in simulation, and furthermore eliminates the numerical sophistication of the system by reducing the proportions of the function while designing the subsequent framework. Such research efforts can be further summarized as follows, first emphasizing the value of rising-dimensional security measures in a deep extreme learning machine-based intrusion detection technique, and then implementing a Deep Extreme Learning Machine-focused intrusion detection system, that initially brings into account the ranking of security parameters for their validity and importance.

The proposed architecture for detecting intrusions therefore in study is therefore built on anomaly centered machine learning techniques. It could also detect novel attacks in this situation. The DELM-based IDS architecture leverages a creative technique to maximize the number of false alerts over span. This is done by providing the freedom to change the training algorithm dependent on recommendations. This eliminates the likelihood of frequent false alarms of similar data in an optimal way. Finally, we conduct analysis to test the effectiveness of our DELM-based IDS system for intrusion detection. Investigational results show that our DELM-based IDS platform immensely outperforms existing solutions for detecting cyber intrusions in various unknown sets of data.

2 Related Works

The Internet of Things (IoT) is transforming communities increasingly into smart cities through offering a new means of living in urban communities. Enhanced health, well-being, higher schooling and living conditions, effective usage of energy, improved environmental and forest conservation, a healthy economy and more employment are main benefits. While the fundamental concept of smart communities has been present for approximately two decades, it has been expected that community life would transform significantly after it was first adopted as a variety of primary mediators, such as the IoT, appeared. Badii et al. [11] concluded that the dream of emerging technologies is safe, secure, sustainable and competitive in all aspects, such as electricity, water and mobility. Aujla et al. [12] clarified that Smart City is a technology-centric and better-connected resident, information and urban amenities by technological advancements, building a healthy, secure climate, a profitable and innovative business, and enhancing standard of living [13]. The smart city has been described as a dynamic community wherein disparate aspects, like the individuals, the climate, governance, government and the infrastructure, are integrated through a digital infrastructure.

An intrusion detection framework is typically used to identify malicious cyber-threats activity on a network by monitoring and evaluating the day-to-day operations in a system or computing system to locate security flaws or threats [14]. Throughout the area of information security, a variety of research has been undertaken to detect and prevent cyber-attacks or infringements. One of the common approaches used in the cybersecurity field is signature-based network intrusion detection [15]. This system carries an existing signature into account and has seen mainstream recognition in recent times, alongside economic development. In the other hand, the anomaly approach benefits from the signature system for detecting unseen attacks, such as the probability of identifying hidden or zero-day assaults [16]. The approach monitors network interaction and recognizes behavioral patterns for risks by analyzing relevant safety details. Various techniques of data mining and deep learning are used to classify such clusters of safety events in order to establish consistency assessments [6]. A main drawback to the anomaly-based approach being that it may produce massive false alarm rates as it would classify unrevealed device activities as anomalies. A big challenge would be to the false positive rate of the intrusion detection method [17]. Nevertheless, an appropriate approach of detection based on machine learning is necessary to alleviate these challenges.

Frameworks for machine learning have gained a lot of interest. Park et al. [1] provided a detailed description of the features of machine learning intrusion detection approaches. Armitage et al. [18] suggested a comprehensive explanation utilizing machine learning, with a focus on the analysis of IP traffic. Bkassiny et al. [19] explored several dynamic information problems in Cognitive Radio Networks and examined emerging machine-based learning approaches. How to solve numerous issues with Machine learning techniques in the wireless networks has been studied in [20]. Wang et al. [21] develop state-of-the-art strategies for developing stratified artificial intelligence (AI) networks, and addressing potential study issues. Guven et al. [16] researched machine learning and data mining approaches for cybersecurity malware detection. Klaine et al. [22] researched and discussed the important description as well as evaluation of machine-learning programs and respective wireless network interpretations. Fadlullah et al. [23] investigate about using machine learning approaches to boost traffic control in networks. Related to [1,24] focus even on an Intrusion Detection System (IDS) centered on machine learning. Zhou et al. [25] demonstrate the usage of artificial intelligence and cognitive radiation skills to boost bandwidth utilization and energy performance in the wireless network. Chen et al. [26] studied neural network-based approaches to wireless network challenges such as convergence, virtual reality and edge cache.

In comparison to the aforesaid approaches, we propose in this research a deep extreme learning machine-based intrusion detection framework that first catches the identification of security concerns according to their importance and then creates a generalized framework for detecting intrusions focused on the defined prominent components to resolve the aforementioned-mentioned problems.

3 System Model

The suggested intrusion detection technology is built in this work on anomaly-based machine learning approaches. It would then be willing to recognize new threats. The suggested DELM base intrusion detection system uses a creative approach to reduce the amount of false warnings over the span. That is accomplished by providing the ability to receive input from human experts and by updating the learning model in conjunction with that knowledge. This eliminates the probability of frequent false warnings of similar details in a successful manner.

Nevertheless, both unsupervised and supervised learning approaches should be addressed for the suggested based intrusion detection system. Resultantly, label data is not needed in the training phase. As the proportion of network segments seems to be the only specific knowledge available, the suggested solution encourages the selection of the suitable labeling for mislabeled data. Instead it provides recommendations for adaptation in situations where the training samples are usually identified by human analysts.

The planned intrusion detection system provides a structure to ease the review of actions made by public protection experts. The system will classify anomalies through predetermining findings via this method. In the supervised structure learning, however, the system has the ability to identify human error when labeling the information and to make feedback to the proposal. At the other edge, the framework will classify new sections of traffic using a scoring method.

In fact, the suggested intrusion prevention system offers a quick updating mechanism that addresses the adaptability problem of current strategies. The suggested architecture will be used to update the learning system on the basis of existing knowledge and, to date, emerging types of attacks with reduced computing costs.

Fig. 1 defines the planned DELM-based intrusion detection method used by the NSL-KDD data collection. The graphical description of our framework is demonstrated in Fig. 1 two structures are employed for intrusion detection operations: a learning algorithm conditioned by a classified array of knowledge and this approach may be used as major aspect of the identification of attacks in the pre-processing layer; a novel system for detecting security threats in certain periods after deep extreme learning machine has been deployed.

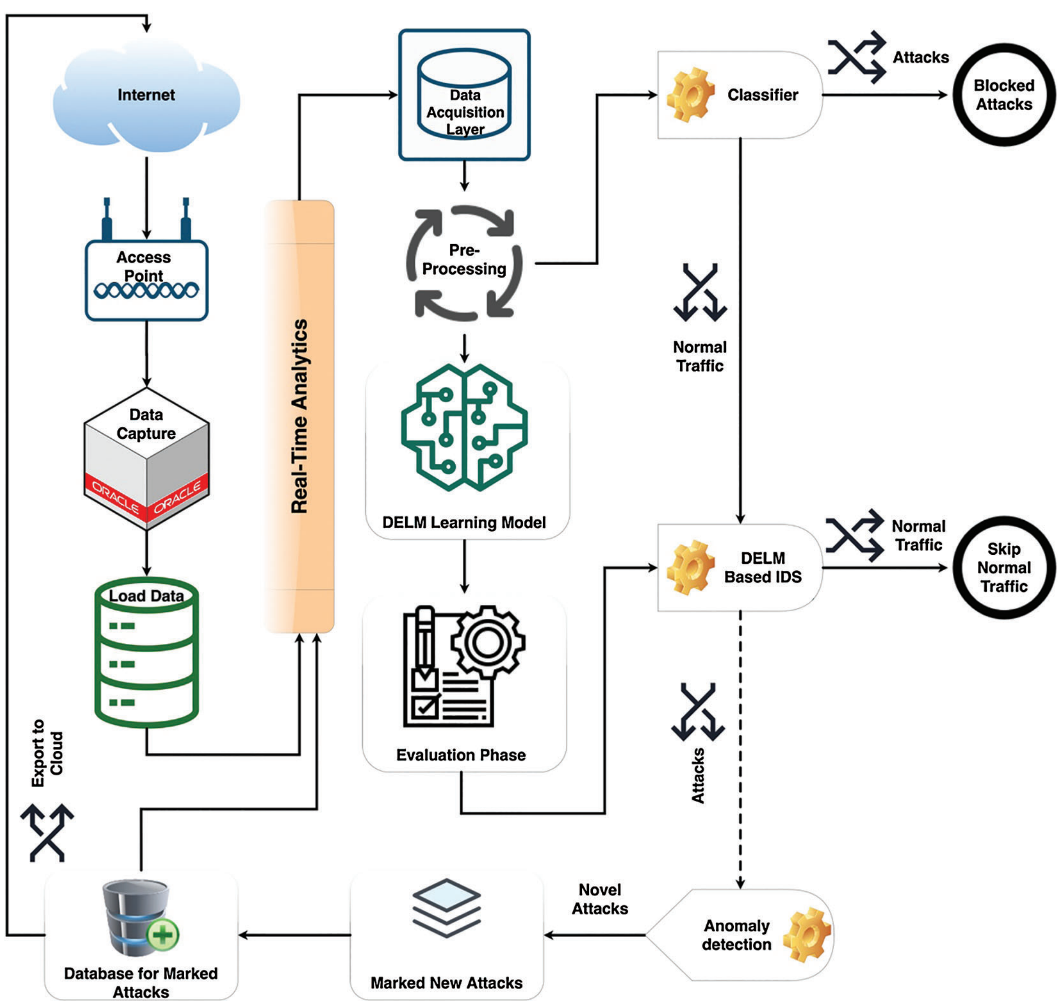

Figure 1: Proposed deep extreme learning machine based intrusion detection system

3.1 Dataset Description

For this analysis, we employed the Kaggle publicly available intrusion data collection that constitutes of dual forms one of which is normal and the other of which is attack [27]. Tab. 1 lists all protection protocols falling under their identity group. The NSL-KDD dataset is a refined edition of KDD 99 that includes several enhancements related to the original KDD 99 data collection [28]. The NSL-KDD data collection contains 41 functions for each record. Tab. 1 offers a proper description of the functions. In addition, every element has a labeling which shows its traffic form. This label could indicate normal or malicious traffic. Viewable threat categories for NSL-KDD information are predicted to collapse as follows to four main levels [27], Denial of service (DoS), Remote to local (R2L), user to root (U2R) and probe. Each of the aforementioned forms of attacks involve several sample attacks in the collection of details.

Table 1: Dataset structure

Features	Form of value	Features	Form of value
Duration	Integer	is_guest_login	Integer
protocol_type	Nominal	count	Integer
Service	Nominal	srv_count	Integer
Flag	Nominal	serror_rate	Float
src_bytes	Integer	srv_serror_rate	Float
dst_bytes	Integer	rerror _rate	Float
land	Integer	srv_rerror_rate	Float
wrong_fragment	Integer	same_srv_rate	Float
urgent	Integer	diff _srv_rate	Float
hot	Integer	srv_diff_host_rate	Float
num_failed_logins	Integer	dst_host_count	Float
root_shell	Integer	dst_host_srv_count	Float
num_compromised	Integer	dst_host_same_srv_rate	Float
roots_hell	Integer	dst_host_diff_srv_rate	Float
su_attempted	Integer	dst_host_same_src_port_rate	Float
num_root	Integer	dst_host_srv_diff_port_rate	Float
num_file_creations	Integer	ddst_host_serror_rate	Float
num_shells	Integer	dst-_host_srv_serror_rate	Float
num_access_files	Integer	dst_host_rerror_rate	Float
num_outbound_cmds	Integer	dst_host_srv_rerror_rate	Float
Is_host_login	Integer		

3.2 Deep Extreme Learning Machine

DELM architecture has an enormous range of hidden layers, often has some hidden neurons, and many forms of activation functions are used to obtain the right configuration for maximizing network security. The suggested structure comprises of three layers, the first layer is the data collection layer, the second one is the pre-processing layer and the third one is the evaluation layer. Two sub-layers are used in the program framework, one for estimation and the other for assessment. Real data was collected from the cloud or database for experimental studies. When data was processed, the data was then transmitted as input to the data collection layer. In the preprocessing step, different data cleaning procedures and examination methods are implemented to remove irregularities from the real data. The Deep extreme learning machine (DELM) architecture is deployed in the application layer in order to increase network security against any disruptive or invasive activity.

The DELM method can be extended to different frameworks for intrusion detection. A large percentage of system parameters are usually needed to maintain the appropriate detection accuracy. DELM minimizes various issues for network developers such as network stability and accessibility. Estimating that 80% of the network's resources is used through data transmission and retrieval, feature extraction and function extraction strategies can be utilized to reduce consumption and increase the lifetime of the network. Owing to excessive computational and memory requirements, widely deployed encoding techniques can lead to increased resource consumption. DELM is reduce the output requirement for information compression across networks. Network security also includes real-time networking strategies involving safety, scheduling, monitoring, grouping networks, collating information, detecting errors and integrity of data. DELM provides a structure that strengthens network security's ability to adapt to the dynamic actions of its circumstances.

The Deep extreme learning machine (DELM) can be implemented in various disciplines to anticipate safety issues, energy use forecasts, transportation and traffic control, etc. [29–31]. Standard artificial neural network frameworks involve a variety of activities and slow learning intervals which may override the learning framework [32]. The definition of an extreme learning machine is termed by Huang et al. [33]. Extreme learning machine algorithm is usually a feed-forward neural network, which means that information travels just one path over a series of layers, but we have also deployed the back-propagation method in this forecasting model throughout the training period, where data streams backward through the network in back-propagation, the neural network changes weights to attain high precision at lowest error. Weights are unchanged throughout the testing process of the network wherein the trained framework is imported and the actual results are expected. If the system has been trained, the trained model exported to the cloud for online usage can be used for testing objectives across the network during the validation process. Mean square error (MSE) is observed in the evaluation layer to improve network security.

DELM incorporates other popular learning techniques, such as Backpropagation while dynamically structuring input weights; DELM only adjusts output weights in one incremental step without adjusting input weights. Thus, it provides a fast and detailed learning capability. The methods of the DELM shall work as follows.

Anticipate that we provide numerous hidden layer feed-forward neural nets n quantity of hidden layer neurons and a training dataset of N samples (e_i, f_i) in which $e_i \in S_d$ and $f_i \in S_c$. The aftermath of these numerous hidden Layer Feedforward Neural network can be signified as;

$$\sum_{j=1}^{n} \gamma_j L \left(\mathrm{z}_j \mathrm{e}_\mathrm{i} + a_j\right), \quad i \in [1, N], \tag{1}$$

Now z_j and a_j are learning variables, γ_j nodes output weight j and $L : S \rightarrow S$ is the activation function.

An appropriate synthesis of numerous hidden Layer Feedforward Neural network with null error reveals this at discrete intervals. z_j and a_j there appear γ_j such that

$$\sum_{j=1}^{n} \gamma_j L\left(z_j e_i + a_j\right) = f_i, i \in [1, N], \tag{2}$$

which could be interpreted as

$$Q\gamma = F, \tag{3}$$

where

$$Q = \begin{bmatrix} L(z_1 e_1 + a_1) & & L(z_n e_1 + a_n) \\ \vdots & & \vdots \\ \vdots & \cdots & \vdots \\ L(z_1 e_N + a_1) & & L(z_n e_N + a_n) \end{bmatrix} \tag{4}$$

and

$$\gamma = \left(\gamma_1^T \ldots \gamma_n^T\right)^T, \quad F = \left(f_1^T \ldots f_N^T\right)^T \tag{5}$$

If the volume of measurements over the hidden layer neurons, the weights of the result can be calculated using the formula below

$$\gamma = Q^{ł}F \tag{6}$$

And $Q^{ł}$ is the inverse of matrix Q. Therefore, DELM is a computationally efficient analysis method.

The backpropagation process includes the adjustment of weights, forward propagation, backward propagation of error, and the upgrading of distinguishability. An activation function like $g(x) = \textit{sigmoid}$ is illustrate in the hidden layer on each neuron. This enables develop the sigmoid input feature and the deep extreme learning machine hidden layer;

$$E = \frac{1}{2}\sum_j \left(sj - wp_j\right)2 \tag{7}$$

sj = Required outcome

wp_j = Computed outcome

Eq. (7) outlines a backpropagation loss, which can be calculated by varying the square amount by 2 from the appropriate value. Weight correction is needed to minimize the that loss. The values of weight shift for the output layer are stated in Eq. (8).

$$\Delta H_{i,j}^{l=6} \propto -\frac{\partial R}{\partial H^{l=6}} \tag{8}$$

$i = 1, 2, 3 \ldots 10(\textit{no.of neurons})$ and j = Layer of Output Value

$$\Delta H_{i,j}^{l=6} = -\text{const}\frac{\partial R}{\partial H^{l=6}} \tag{9}$$

Write Eq. (9) through the chain rule procedure;

$$\Delta \mathrm{H}_{i,j}^{l=6} = -\mathrm{const}\frac{\partial \mathrm{R}}{\partial wp_j^l} \times \frac{\partial wp_j^l}{\partial NhH_j^l} \times \frac{\partial NhH_j^l}{\partial H_{i,j}^l} \tag{10}$$

The variation in weight value can be attained by interchanging the values in Eq. (14) as indicated in Eq. (10).

$$\Delta H_{i,j}^{l=6} = \mathrm{const}\left(\mathrm{sj} - wp_j\right) \times \left(wp_j^l \left(1 - wp_j^l\right) \times wp_j^l\right) \tag{11}$$

From wp to H_6

$$\Delta H_{i,j}^{l=6} = \mathrm{const}\,\ni_j wp_j^l \tag{12}$$

The calculation of the corresponding weight change between hidden layer weights is experienced in the next segment. This is consequently complex, since it leads to miscalculations on each node by weighting the relationship.

From H_6 to H_1 or H_n

where $n = 5, 4, 3, 2, 1$

$$\Delta \mathrm{H}_{i,n}^l \propto -\left[\sum_j \frac{\partial \mathrm{R}}{\partial \mathrm{wp}_j^l} \times \frac{\partial \mathrm{wp}_j^l}{\partial \mathrm{NhH}_j^l} \times \frac{\partial \mathrm{H}_j^l}{\partial \mathrm{wp}_n^l}\right] \times \frac{\partial \mathrm{wp}_n^l}{\partial \mathrm{NhH}_n^{hl}} \times \frac{\partial \mathrm{NhH}_n^l}{\partial \mathrm{H}_{i,n}^l} \tag{13a}$$

$$\Delta \mathrm{H}_{i,n}^l = R\left[\sum_j \ni_j (H_{n,j}^l)\right] \times \mathrm{wp}_n^l \left(1 - \mathrm{wp}_j^l\right) \times Z_{i,n} \tag{13b}$$

$$\Delta \mathrm{H}_{i,n}^l = R \ni_n Z_{i,n} \tag{13c}$$

where

$$\ni_n = \left[\sum_j \ni_j (H_{n,j}^l)\right] \times wp_n^l \left(1 - wp_n^l\right) \tag{13d}$$

The function is to improve the weights defined and therefore the bias among the performance and the hidden layer is seen in Eq. (13e).

$$H_{i,j}^{l=6}(t) = H_{i,j}^{l=6}(t) + \lambda \Delta H_{i,j}^{l=6} \tag{13e}$$

Eq. (14) Demonstrate the updating of weights and how differences exist among hidden layers and inputs.

$$H_{i,n}^l(t) = H_{i,n}^l(t+1) + \lambda \Delta H_{i,j}^l \tag{14}$$

4 Results and Discussion

In this proposed approach, the NSL-KDD dataset was applied with a deep extreme learning machine framework [27]. The dataset was arbitrarily split into 70% of the training (103962 records), 30% of the dataset were used for validation (44554 records). Data was processed in order to eliminate data anomalies and to reduce errors from dataset. DELM further sought to detect some disruptive or interference in different hidden layers, like hidden neurons, and activation functions. So, we analyzed a range of neurons in hidden layers in the network and even integrated a range of active function forms. Within this study, we evaluate the DELM within order to better estimate the performance of this method. In order to quantify the performance with the predecessor methods with DELM algorithm, we have also used various statistical measures mentioned in Eqs. (15) and (16).

The effectiveness of the experiments performed by the proposed IDS based DELM is measured in this study. The two commonly employed in the field of intrusion detection mechanisms are Detection Level and False Positive Rating, which can be defined in Eqs. (17) and (18);

$$\text{Miss rate} = \frac{\sum_{k=0}^{2}\left(\frac{O_k}{T_{j\neq k}}\right)}{\sum_{k=0}^{2}(T_k)}, \quad \text{where j} = 0, 1, 2 \tag{15}$$

$$\text{Accuracy} = \frac{\sum_{k=0}^{2}\left(\frac{O_k}{T_k}\right)}{\sum_{k=0}^{2}(T_k)} \tag{16}$$

$$\text{Detection Rate} = \frac{\text{Number of Intrusions Detection}}{\text{Total Number of Infused Intrusions}} \tag{17}$$

$$\text{False Positive Rate} = \frac{\text{Generic number of trends categorized as intrusions}}{\text{The overall number of standard patterns}} \tag{18}$$

In Eqs. (17) and (18), O epitomize the prognostic outcome value of DELM based IDS and T epitomize the actual outcome value. O_0 and T_0 epitomizes that there is normal/no attack found in prognostic outcome and actual outcome simultaneously. O_1 and T_1 epitomizes the attack are found in prognostic outcome and actual outcome simultaneously. $\frac{O_k}{T_k}$ epitomizes prognostic and actual outcome values are identical. Similarly, $\frac{O_k}{T_{j\neq k}}$ epitomizes error, where prognostic and actual outcome value diverges.

Tab. 2 displays the planned DELM-IDS for the estimation of intrusion detection during the training process. Overall 103962 records are employed during training, that is subsequently split into 53937, 50025 normal & attack samples, correspondingly. It is noted that 50198 records of normal category mean under which no attack is correctly predicted and 3739 records are incorrectly predicted as an attack detected where there is no real attack. In the same manner, a minimum of 50025 records are performed in the case of an attack detected, of which 45498 records are accurately predicted as an attack identified, and 4527 samples are incorrect forecast as normal, while an attack currently occurs.

Table 2: Training of the proposed deep extreme learning machine-based intrusion detection system during the prediction of malicious attack

Proposed DELM based IDS (70% of sample data in training)			
Total No of samples (N = 103962)		Result (output) (O_0, O_1)	
Input	Expected output (T_0, T_1)	O_0 (Normal)	O_1 (Attack)
	T_0 = 53937 Normal	50198	3739
	T_1 = 50025 Attack	4527	45498

Tab. 3 displays the planned DELM-IDS for the estimation of intrusion detection during the validation process. Overall 44554 records are employed during training, that is subsequently split into 23116, 21438 normal & attack samples, correspondingly. It is noted that 21503 records of normal category mean under which no attack is correctly predicted and 1613 records are incorrectly predicted as an attack detected where there is no real attack. In the same manner, a minimum of 21438 records are performed in the case of an attack detected, of which 19144 records are accurately predicted as an attack identified, and 2294 samples are incorrect forecast as normal, while an attack currently occurs.

Table 3: Validation of the proposed deep extreme learning machine-based intrusion detection system during the prediction of malicious attack

Proposed DELM based IDS (30% of sample data in validation)			
Total No. of samples (N = 44554)		Result (output) (O_0, O_1)	
Input	Expected output (T_0, T_1)	O_0 (Normal)	O_1 (Attack)
	T_0 = 23116 Normal	21503	1613
	T_1 = 21438 Attack	2294	19144

Tab. 4 displays the suggested DELM-based IDS findings in aspects of accuracy & miss rate across the training & validation process. It is explicitly observed that the proposed IDS based DELM during training offers 92.04% & 7.96% accuracy and miss rates, correspondingly. And during validation, the suggested DELM based IDS offers 91.23% & 8.77% accuracy & miss rate, correspondingly.

Table 4: Performance evaluation of proposed deep extreme learning machine-based intrusion detection system during validation & training

	Accuracy	Miss rate
Training	92.04%	7.96%
Validation	91.23%	8.77%

We compared the performance of our method with the existing NSL-KDD dataset methodologies. As shown in Tab. 5, with a lower error rate, the suggested system accomplishes significantly excellent accuracy. The proposed DELM methodology is attractive to other versions in terms of precision, such as the SVM [28], Self-Organization Map [34], ANN-based IDS [35], Discriminative multinomial Naïve Bayes [36] and Generative Adversarial Networks [37]. The performance of the DELM method increased efficiency over the NSL-KDD data set. In contrast with other machine learning approaches, the accuracy of the support vector machine (SVM) [28] is much lower. In [36], the authors projected Discriminative Multinomial Naïve Bayes with Random Projection and in this technique, the researchers attained 81.47% accuracy. In [34], the researchers projected Self-Organization Map and, in this technique, the researchers attained 75.5% accuracy. In [35], the researchers projected an ANN-based IDS and, in this technique, the researchers attained 81.2% accuracy. In [37], the researchers projected Generative Adversarial Networks (GANs) and in this technique, the researchers attained 86.5% accuracy. The estimated accuracy of the DELM method is 91.23% and better in terms of consistency than the approaches previously introduced.

The suggested efficiency of the DELM system is considerably better than other approaches focused on methodological values. The proposed DELM-based IDS architecture is therefore a considerable choice for an intelligent network security solution.

Table 5: Comparison results of the proposed deep extreme learning machine-based intrusion detection system with literature

Method	Accuracy rate
SVM [28]	69.5%
Self-organization map [34]	75.5%
ANN based IDS [35]	81.2%
Discriminative multinomial Naïve Bayes [36]	81.5%
GANs [37]	86.5%
Deep extreme learning machine (proposed)	91.23%

5 Conclusion

In this research, we suggested a deep extreme learning machine-based intrusion detection framework. Firstly, we mention the security features according to their importance and then we construct a generalized intrusion detection model based on the relevant features observed. We also done this to make the security model effective and competitive by growing computing difficulty for predicting precision for uncertain data sets. Ultimately, by running a series of data set experiments, we measured the efficiency of our DELM based IDS. To assess the viability of the suggested solution, different analytical methods were employed. These evaluating results demonstrate that the DELM based IDS solution suggested is far more reliable than other approaches. The suggested IDS security framework concentrated on DELM provide promising results. The suggested method demonstrates 96.22% and 92.73% precision through training and validation, respectively. We have compared the results of the DELM-based IDS system with other traditional standard methods for evaluating the effectiveness of the related security architecture.

Acknowledgement: Thanks to our families & colleagues who supported us morally.

Funding Statement: This Work is supported by Data and Artificial Intelligence Scientific Chair at Umm AlQura University.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[2] N. Sun, J. Zhang, P. Rimba, S. Gao, L. Y. Zhang *et al.*, "Data-driven cybersecurity incident prediction: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1744–1772, 2019.

[3] A. Dainotti, A. Pescape and G. Ventre, "Worm traffic analysis and characterization," in *IEEE Int. Conf. on Communications*, Glasgow, UK, pp. 1435–1442, 2007.

[4] X. Qu, L. Yang, K. Guo, L. Ma, M. Sun *et al.*, "A survey on the development of self-organizing maps for unsupervised intrusion detection," *Mobile Networks and Applications*, vol. 13, no. 2, pp. 1–22, 2019.

[5] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proc. of the 6th annual Int. Conf. on Mobile Computing and Networking*, Chicago, Illinois, USA, pp. 275–283, 2000.

[6] C. F. Tsai, Y. F. Hsu, C. Y. Lin and W. Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications*, vol. 36, no. 10, pp. 11994–12000, 2009.

[7] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li *et al.*, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.

[8] L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[9] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques," *Procedia Computer Science*, vol. 60, pp. 708–713, 2015.

[10] H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters *et al.*, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, pp. 1–29, 2020.

[11] C. Badii, P. Bellini, A. Difino and P. Nesi, "Smart city IoT platform respecting GDPR privacy and security aspects," *IEEE Access*, vol. 8, pp. 23601–23623, 2020.

[12] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han *et al.*, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Network*, vol. 32, no. 2, pp. 83–91, 2020.

[13] S. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh *et al.*, "Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward," *IEEE Access*, vol. 8, pp. 474–488, 2020.

[14] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," *ACM Computing Surveys*, vol. 48, no. 1, pp. 1–41, 2015.

[15] S. Seufert and D. O'Brien, "Machine learning for automatic defence against distributed denial of service attacks," in *2007 IEEE Int. Conf. on Communications*, Chicago, Illinois, USA, pp. 1217–1222, 2007.

[16] L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[17] R. Sommer and V. Paxson, "Outside the closed world: on using machine learning for network intrusion detection," in *2010 IEEE Sym. on Security and Privacy*, Chicago, Illinois, USA, pp. 305–316, 2010.

[18] T. T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE Communications Surveys Tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

[19] M. Bkassiny, Y. Li and S. K. Jayaweera, "A survey on machine- learning techniques in cognitive radios," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1136–1159, 2013.

[20] M. A. Alsheikh, S. Lin, D. Niyato and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014.

[21] X. Wang, X. Li and V. C. M. Leung, "Artificial intelligence-based techniques for emerging heterogeneous network: state of the arts, opportunities, and challenges," *IEEE Access*, vol. 3, pp. 1379–1391, 2015.

[22] P. V. Klaine, M. A. Imran, O. Onireti and R. D. Souza, "A survey of machine learning techniques applied to self organizing cellular networks," *IEEE Communications Surveys & Tutorials*, vol. 99, no. 4, pp. 2392–2431, 2017.

[23] Z. M. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi *et al.*, "State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432–2455, 2017.

[24] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," *ArXiv Preprint ArXiv*, vol. 17, no. 1, pp. 1–43, 2017.

[25] X. Zhou, M. Sun, G. Y. Li and B. H. Juang, "Machine learning and cognitive technology for intelligent wireless networks," *ArXiv Preprint ArXiv*, vol. 2017, pp. 1–53, 2017.

[26] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, "Machine learning for wireless networks with artificial intelligence: A tutorial on neural networks," *ArXiv Preprint ArXiv*, vol. 17, no. 10, pp. 1–93, 2017.

[27] Hassan, Kaggle, 2020. [Online]. Available: https://www.kaggle.com/hassan06/nslkdd.

[28] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in *2009 IEEE Sym. on Computational Intelligence for Security and Defense Applications*, Chicago, Illinois, USA, pp. 1–6, 2009.

[29] S. Abbas, M. A. Khan, L. E. Falcon-Morales, A. Rehman, Y. Saeed *et al.*, “Modeling, simulation and optimization of power plant energy sustainability for IoT enabled smart cities empowered with deep extreme learning machine,” *IEEE Access*, vol. 8, pp. 39982–39997, 2020.

[30] A. Rehman, A. Athar, M. A. Khan, S. Abbas, A. Fatima *et al.*, “Modelling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine,” *Journal of Ambient Intelligence and Smart Environments*, vol. 12, no. 2, pp. 125–138, 2020.

[31] M. A. Khan, S. Abbas, K. Masood Khan, M. A. Ghamidi and A. Rehman, “Intelligent forecasting model of COVID-19 novel coronavirus outbreak empowered with deep extreme learning machine,” *Computers, Materials & Continua*, vol. 64, no. 3, pp. 1329–1342, 2020.

[32] C. Jiatan, “QAPSO-BP algorithm and its application in vibration fault diagnosis for a hydroelectric generating unit,” *Journal of Vibration and Shock*, vol. 34, no. 23, pp. 177–181, 2015.

[33] G. Huang, D. Wang and Y. Lan, “Extreme learning machines: A survey,” *International Journal of Machine Learning and Cybernetics*, vol. 2, no. 2, pp. 107–122, 2011.

[34] L. M. Ibrahim, D. T. Basheer and M. S. Mahmod, “A comparison study for intrusion database (Kdd99, Nsl-Kdd) based on self organization map (SOM) artificial neural network,” *Journal of Engineering Science and Technology*, vol. 8, no. 1, pp. 107–119, 2013.

[35] B. Ingre and A. B. Yadav, “Performance analysis of NSL-KDD dataset using ANN,” in *Int. Conf. on Signal Processing and Communication Engineering Systems*, Guntur, India: IEEE, pp. 92–96, 2015.

[36] M. Panda, A. Abraham and M. R. Patra, “Discriminative multinomial Naïve Bayes for network intrusion detection,” in *Sixth Int. Conf. on Information Assurance and Security*, Atlanta, GA, USA, pp. 5–10, 2010.

[37] R. Alshinina and K. Elleithy, “A highly accurate machine learning approach for developing wireless sensor network middleware,” in *2018 Wireless Telecommunications Sym.*, Phoenix, AZ, pp. 1–7, 2018.