Computers, Materials & Continua
DOI:10.32604/cmc.2022.020173
Article

Tech Science Press

Data Fusion-Based Machine Learning Architecture for Intrusion Detection

Muhammad Adnan Khan[1], Taher M. Ghazal[2,3], Sang-Woong Lee[1,*] and Abdur Rehman[4]

[1]Pattern Recognition and Machine Learning Lab, Department of Software, Gachon University, Seongnam, 13557, Korea
[2]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebansaan Malaysia (UKM), 43600, Bangi, Selangor, Malaysia
[3]School of Information Technology, Skyline University College, University City Sharjah, 1797, Sharjah, UAE
[4]School of Computer Science, National College of Business Administration & Economics, Lahore, 54000, Pakistan
[*]Corresponding Author: Sang-Woong Lee. Email: slee@gachon.ac.kr
Received: 12 May 2021; Accepted: 29 June 2021

Abstract: In recent years, the infrastructure of Wireless Internet of Sensor Networks (WIoSNs) has been more complicated owing to developments in the internet and devices' connectivity. To effectively prepare, control, hold and optimize wireless sensor networks, a better assessment needs to be conducted. The field of artificial intelligence has made a great deal of progress with deep learning systems and these techniques have been used for data analysis. This study investigates the methodology of Real Time Sequential Deep Extreme Learning Machine (RTS-DELM) implemented to wireless Internet of Things (IoT) enabled sensor networks for the detection of any intrusion activity. Data fusion is a well-known methodology that can be beneficial for the improvement of data accuracy, as well as for the maximizing of wireless sensor networks lifespan. We also suggested an approach that not only makes the casting of parallel data fusion network but also render their computations more effective. By using the Real Time Sequential Deep Extreme Learning Machine (RTS-DELM) methodology, an excessive degree of reliability with a minimal error rate of any intrusion activity in wireless sensor networks is accomplished. Simulation results show that wireless sensor networks are optimized effectively to monitor and detect any malicious or intrusion activity through this proposed approach. Eventually, threats and a more general outlook are explored.

Keywords: Wireless internet of sensor networks; machine learning; deep extreme learning machine; artificial intelligence; data fusion

1 Introduction

Today's network environments have become more and more heterogeneous, and we now must configure network flow and monitor a larger variety of devices [1]. But due to the strict requirement of conventional centralized networks, learning methods are difficult to be applied and used in the management and governance of wireless sensor networks. There are numerous integrated devices in wireless sensor networks, such as low-cost sensors, a microphone to get multimedia information from the area, such as video streams, audio streams, and scalar sensor data. In

general, a production network uses many devices, runs several protocols, and supports several applications [2]. Data transmission has been growing exponentially in the world recently with the rapid evolution of smart devices and network technologies (for example, cloud computing and virtualization of networks) [3]. In the case of wireless networks, several different kinds of cellular transmitting methods have been implemented for a certain spectrum, a transmission capacity, with certain hardware, and the transmission technologies. These approaches expand upon existing efforts by including much more accountability in networks [4]. Cognitive and machine learning integration methods are used to widen the scope of automation, provide guidance, and use it to apply expertise in an internet-based framework [5]. The main reason is that the conventional network networks are fundamentally distributed when only small parts of the network can be accessed and managed by every node such as a router or switch. It is extraordinarily difficult to navigate the whole network by learning from nodes that have a slight, minimal impact on the vast network [6]. Fortunately, current advances in the field of wireless sensor networks will facilitate learning complexity.

Initially, Wireless Sensor Networks (WSNs) that gather the dispersed information, and edge computing enables the effectiveness of conventional sensor networks [7]. Wireless multimedia sensor networks are a new type of network integrating video, audio, images, and other multimedia processing functions that are based on conventional Wireless Sensor Networks (WSNs) [8,9]. Wireless Sensor Networks (WSNs) interpret different media data through multimedia sensor nodes in their surroundings. These data may be sent via a singular and a multi-hop relay to the selected nodes. Compilation nodes interpret and evaluate the collected data and send the review and intervention reports for detailed and efficient environmental monitoring to the network owner. Wireless Sensor Networks (WSNs) are adapted and applied to conventional Wireless Sensor Networks (WSNs) and used frequently for defense and climate protection, intelligent transport and residences, etc. Wireless Sensor Networks (WSNs) are a standard technology that is inspired by the Wireless Sensor Networks (WSNs) and edge computing combination. Internet of Things (IoT) will be the most powerful method to render communities safer [10]. To render Internet of Things (IoT) smart, several innovations and techniques of computing are often used in Internet of Things (IoT) [11].

Earlier studies on neural networks hypothesized that cognitive agents used the best resources available to achieve improve performance [12–14]. The primary principle in this research project is the optimization of Wireless Sensor Networks (WSNs) to apply complex mechanisms for tracking a network malicious activity or protocol violations. This article summarizes wireless sensor networks and smart network challenges and then describes a cohesive structure for improving wireless sensor networks. The Real-Time Deep Extreme Learning Machine (RTS-DELM) approach would be used to make wireless sensor networks more stable and perform better. Safe and effective architectures pervade smart cities, incorporating sophisticated management systems and demand-responsive policies [15].

Wireless Sensor Networks (WSNs) provide a separation of the control and data planes. The Networking operating system, which acts as a technically centralized controller, manages the network infrastructure in Wireless Sensor Networks (WSNs). Wireless Sensor Networks (WSNs) must flexibly administer the network. Moreover, by collecting and tracking network status and initialization data in addition to packet and flow size data, the centralized controller has an overall assessment of the network.

For these purposes, it is necessary and effective to incorporate Wireless Sensor Networks (WSNs) machine learning techniques. To begin, consider the recent advancements in computer

technology, including Graphics Processing Unit (GPU) and the Tensor Processing Unit (TPU), which offer a good chance of using exciting machine learning strategies in the field of networking [16,17]. Second, information is the fundamental need of the learning algorithms of data-driven machines. The main Wireless Sensor Networks (WSNs) have a worldwide network view and gather different network details to simplify applications for machine learning algorithms. Thirdly, machine learning techniques can include Wireless Sensor Networks (WSNs) expertise based on data collection, network configuration, and effective network service delivery based on empirical and legitimate network details. Finally, using machine-learning algorithms, Wireless Sensor Networks (WSNs) technology enables the application of advanced system integration (for example, setup and resource allocation) in real-time on the network [18]. In this article, we discuss the better approach for the production and implementation of machine training in Wireless Sensor Networks (WSNs). The study focuses on machine learning strategies for enhanced performance, intelligence, safety, and reliability of the Wireless Sensor Networks (WSNs) and offers a brief overview of future research recommendations with sufficient scope and breadth in the associated areas. A roadmap is provided for our methodology in Fig. 1.

The Real-Time Deep Extreme Learning Machine (RTS-DELM) is capable of automating data analytics processes and generating real-time analytics. The datasets being evaluated by the Real-Time Deep Extreme Learning Machine (RTS-DELM) system will be evaluated in Wireless Sensor Networks (WSNs), which eliminates all imperfections. Networks need stable data. We would disregard any data-related challenges in the Real-Time Deep Extreme Learning Machine (RTS-DELM) system. It will include a specific mechanism to track and anticipate potential fraud and other illegal activity. In this paper, a real-time deep extreme learning machine-based model is investigated for the intelligent prediction of intrusion detection in wireless sensor networks, which attain the utmost precision. In the training and testing of intrusion detection in Wireless Sensor Networks (WSNs) optimization with real-time deep extreme learning machine, a fused dataset (NSL-KDD and KDD CUP 99) with 47840 data samples are analyzed, so that every instance has specific and varied features. The analysis and contrast with the best techniques are therefore performed in the same area.

In complex networks, the use of data fusion methods can be a benefit due to the huge number of messages shared, as a data fusion task can combine many messages invaluable and accurate data for the final consumer. In this article, we introduce a method for data fusion in networks that naturally scales to large numbers of nodes. In the latest research literature, numerous methods and concepts are used for data fusion. Two of the most widely used classifications are “data fusion” and “information fusion”. In our study, we concentrate only on data reported from sensors, and not on data generated from any other inputs. In a data fusion strategy, sensors are used in tandem to increase the accuracy of decisions.

Finally, this article is structured into the following parts. Section 2 concisely explains the literature. Section 3 describes the methodology for carrying out a thorough assessment. Section 4 describes the Real-Time Deep Extreme Learning Machine (RTS-DELM) method. Section 5 of the paper addresses the simulation and the output effects of the Real-Time Deep Extreme Learning Machine (RTS-DELM) method. Section 6 consists of the explanation and conclusions.

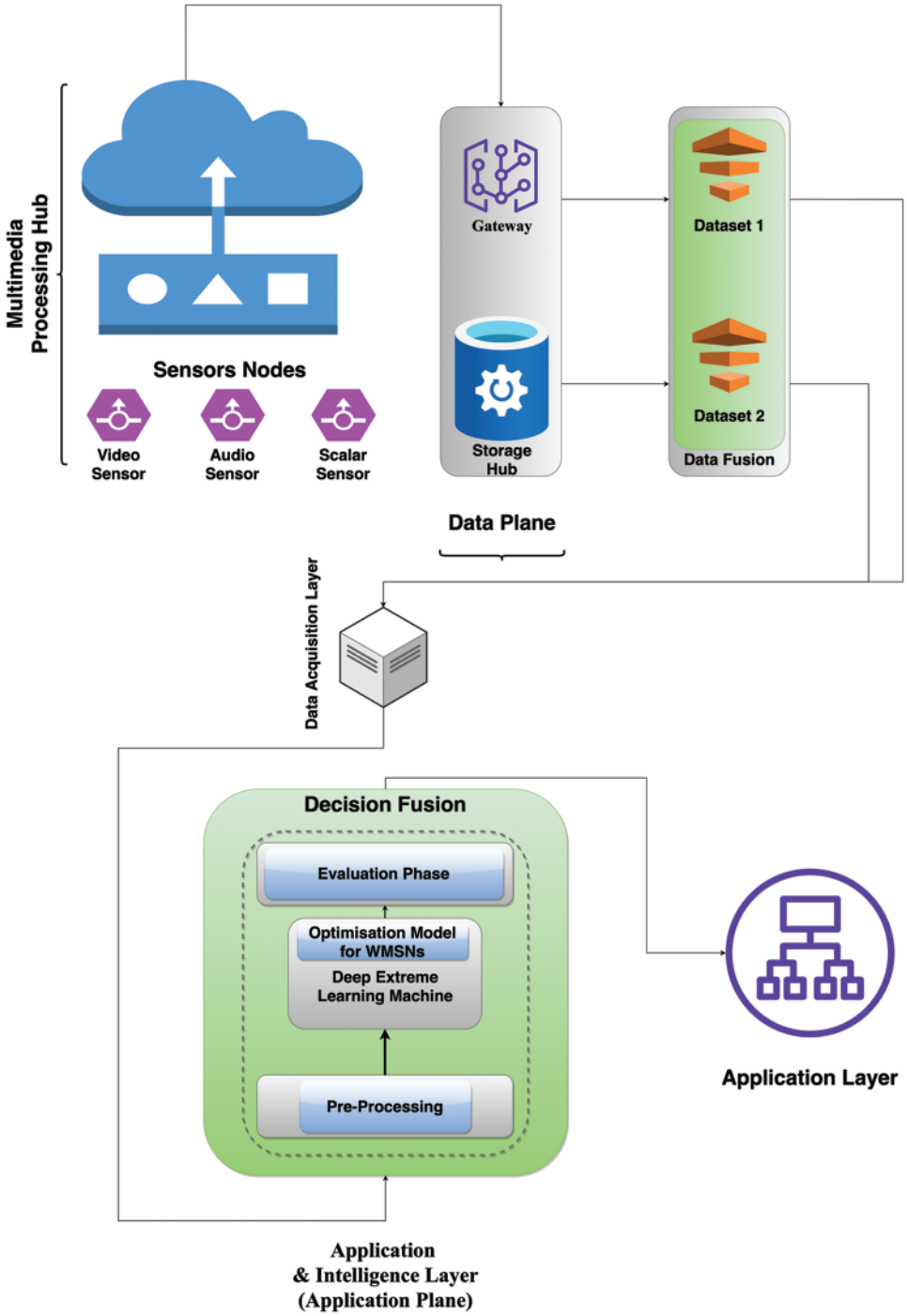

Figure 1: Proposed model for data fusion technique for analysis of intrusion detection for wireless internet of sensor networks using Real-Time Deep Extreme Learning Machine (RTS-DELM)

2 Related Work

In Wireless Sensor Networks (WSNs), the data rate, energy usage, and transmission gap are typically influenced by the deployed system resulting in high rates of ambiguity. The Type-2 fuzzy logic system (T2FLS) approach of Transmission power allocation (TPA) will easily accomplish an alignment among latency and energy consumption and can enhance the network existence of Wireless Sensor Networks (WSNs). Ahmed et al. [19] gives a detailed overview of the roles of high-accuracy intrusion detection machine learning methods. Nguyen et al. [20] proposed systematic coverage of the essence and role of various methods of detecting malware. Bkassiny et al. [21] have learned several complex topics in cognitive radio networks and explored different machine learning-based methodologies. The numerous problems that exist in wireless sensor networks have now been researched in [22]. Wang et al. [23] explores emerging approaches for designing various networks in artificial intelligence. Buczak et al. [24] carried out an in-depth analysis of data mining and intrusion detection methodologies and their concerns. Klaine et al. [25] researched and explained a valuable identification and association of machine-learning frameworks with interpretations of wireless services. Fadlullah et al. [26] examines the potential of machine learning techniques to further strengthen network management. Related to Ahmed et al. [19], Hodo et al. [27] concentrate also on the machine learning-based Intrusion detection system (IDS). Zhou et al. [28] utilizes machine intelligence and cognitive radio techniques to enhance the overall network output. Chen et al. [29] has conducted studies with regards to networks that include topics like networking, virtual assistance, and edge computing to figure out their best approach.

Reducing energy use and increasing the efficiency of Multi-Radio Wireless Sensor Networks (WSNs) is essential. PSO-based optimization energy-consumption task scheduling seeks out the best possible solution to certain issues of enhancement and might significantly enhance a multi-radio node power consumption and extend the lifespan of the network [30,31]. Building a Cognitive internet of things (CIoT) architecture is a research effort extended to use in developing cognitive solutions for the Internet of things (IoT) devices [32]. Vlacheas et al. [33] suggested a cognitive control scheme whereby autonomous objects could take on more human-like features and roles. Eckert et al. [34] estimates that by the year 2050, three-quarters of the global population will live in cities. The smart idea is seen as a means to achieve warmth in life. The Smart City project uses a range of innovations to make the lives of city residents simpler. Smart cities enhance the climate, as well as provide people with preferred services [35]. Urban and industrial ecosystems can be successfully built by the correct use of information and its delivery [36]. The Internet of Things (IoT) involves several different types of gadgets, as well as cars, smartphones, and enables the communication and transfer of data between them and applications, controls, cameras, appliances, and other objects, and also between people's possessions and the organization's networks [37]. Data mining methods should be prepared to capture information and knowledge as well as machine learning techniques should be capable of gathering data to support and study the various forms of data loss [38–42]. More recent work emphasizes the role of opportunistic networking in successful organizations [43,44].

Wireless Sensor Networks (WSNs) have been effective in a variety of organizations, the splitting of the control plane and data plane is apt to introduce a slew of risks and uncertainties to the Wireless Sensor Networks (WSNs) infrastructure [45]. Therefore, Wireless Sensor Networks (WSNs) can be sensitive to various attacks on the network, including volumetric ones, SYN floods, specific service breaches, and Denial of service (DoS) attacks. These occurrences will push security concerns into the layers of Wireless Sensor Networks (WSNs). There are numerous safety mechanisms used for detecting and mitigating DoS attacks on the SDN network, as discussed

in [46]. These approaches are dependent on the selection of packet flow features. The monitoring packages for harmful activity are bigger than the previously established limit or decision-making limit [47]. Steady information development and the huge numbers of packets that can be handled in real-time are the key disadvantages.

The main contributions of the work are following:

(a) The primary objective is to minimize the miss rate and improve the accuracy of intrusion detection in wireless internet of sensor networks.
(b) For a better approximation of intrusion detection empowered with fused data in wireless sensor networks, a new variant of DEML named Real-Time Deep Extreme Learning Machine (RTS-DELM) has been proposed.
(c) Finally, Simulation results have shown that the suggested fused data based Real-Time Deep Extreme Learning Machine (RTS-DELM) framework is better as compare to other algorithms in terms of accuracy and miss rate such as support vector machine [48], self-organization map [49], artificial neural network-based intrusion detection system [50], discriminative multinomial naïve bayes [51] and Generative adversarial networks (GANs) [52].

3 Proposed System Model

The multiphase WIoSNs architecture is a high-level definition describing three key planes: the multimedia processing core, the data plane, and the application layer. The architectural elements and relationships of each plane are shown in Fig. 1. The multimedia processing hub is the lowest layer of WIoSNs architecture and is also denoted as the infrastructure plane. This plane consists of sensor devices including video, audio, and scalar sensors. Those multimedia processing hubs are responsible for the delivery, drop, and modification of media on the data plane. The data plane is connected through a storage hub, with which the sensors store the data and send data for processing to the proposed framework. The data plan is the core of WIoSNs that can configure network infrastructure, dynamically alter security laws, and make network management flexible and adaptive. A logically central data plane that governs the interaction among transmitting units and applications is the key component of the data network. The data plane is the master node where all data gathers into a storage hub and then multiple datasets are sent to the next plane that performs the data fusion operation. Then fused dataset was sent to the application layer.

In this manner, the NSL-KDD [53] and KDD CUP 99 [48] data set were used for the data fusion technique to test the performance of the proposed system. In the fused data collection, each data defines a specific link corresponding to a series of TCP packets that flow inside a predetermined protocol among the source and destination IP addresses. This data set includes 41 per record number of features. Such characteristics comprise six discrete fields and 35 continuous fields. The performance of four variants of a back-propagation training algorithm on the prediction of defect-prone software modules, followed by the selection of a highly effective training algorithm by using a fuzzy layer, is analyzed and compared using the proposed framework.

4 Real-Time Deep Extreme Learning Machine (RTS-DELM)

An ANN is an interconnected set of units called neurons. Fig. 2 shows different numbers of hidden layers, several hidden neurons, and various kinds of activation functions in Real-Time Deep Extreme Learning Machine (RTS-DELM) to obtain the perfect Real-Time Deep Extreme Learning Machine (RTS-DELM) system for optimizing wireless sensor networks. The suggested architecture is composed of three layers: the data collection layer, the pre-processing layer, and the

implementation layer. A different aspect of the application layer includes two modes of prediction, and the second mode of application serves to examine the results of the current model's predictions. Sensor data is used to collect data for exploratory experiments. After collecting sensor data, it was distributed data acquisition layer. In the pre-processing layer, various information clean-up processes and verification approaches are used to eliminate anomalies from the individual data. The Real-Time Deep Extreme Learning Machine (RTS-DELM) was used to optimize wireless sensor networks to avoid disruptive or invasive behavior.

The Real-Time Deep Extreme Learning Machine (RTS-DELM) approach can be applied to several WSN applications. To preserve the required detection precision, a huge proportion of sensor measurements are normally necessary. Real-Time Deep Extreme Learning Machine (RTS-DELM) mitigates various network access issues by deploying integrated network routing and security features. Considering that 80% of the network's energy is used when transmitting and receiving data, data reduction and function abstraction techniques may minimize processing time and bring durability to neural networks. The overuse of compression techniques will cause a rise in energy costs. Real-Time Deep Extreme Learning Machine (RTS-DELM) allows more effective data compression within Wireless Sensor Networks (WSNs). As a consequence, wireless sensor networks need real-time networking solutions such as security, scheduling, monitoring, clustering nodes, aggregation of data, and fault diagnosis. The Real-Time Deep Extreme Learning Machine (RTS-DELM) architecture lets wireless sensor networks seamlessly respond to their surroundings' dynamic behavior.

The Real-Time Deep Extreme Learning Machine (RTS-DELM) [54] can be employed in many applications and domains to predict health issues, calculates the level of energy usage, inventories services, and stipulates transport operations [55–57]. The standard ANN system involves trials and error, slow learning, and constant overwriting [58]. An extreme learning machine design is implemented by Huang et al. [59]. The Real-Time Deep Extreme Learning Machine (RTS-DELM) can be used to categorize and regress dedicate in various sense as it is simple to understand and efficient at the pace of sophistication of frameworks. A feed-forward neural network is typically learning only in one direction, but in our process, the back-propagation technique is also employed, which involves using the input to adjust the network's weights such that it can attain the greatest accuracy while incurring the lowest possible error. The Real-Time Deep Extreme Learning Machine (RTS-DELM) model includes the input layer, multiple secret layers, and at least one output layer. If the system has been conditioned, this framework is transferred to the cloud for online usage, then it was used for validation services this way across the cloud during the validation process. The Real-Time Deep Extreme Learning Machine (RTS-DELM) extended version of the DELM description is demonstrated in the hierarchical context in Fig. 2.

In the evaluation layer, the Mean square error (MSE) was reviewed for the optimization of wireless sensor networks.

Let's say there are several concealed complex basic Feedforward sequential neural networks with n amount of hidden layer neurons and a training dataset of Y records $(\ni_i, f_i)$ in which $\ni_i \in \S_d$ and $f_i \in \S_c$. The implementation of several hidden layer feed-forward neural networks results in the observed outcome is;

$$\mathrm{f}_i = \sum_{j=1}^{n} ß_j ç\left(\mathrm{ч}_j \ni_\mathrm{i} + \mathrm{ч}_j\right) \; i \in [1, Y] \tag{1}$$

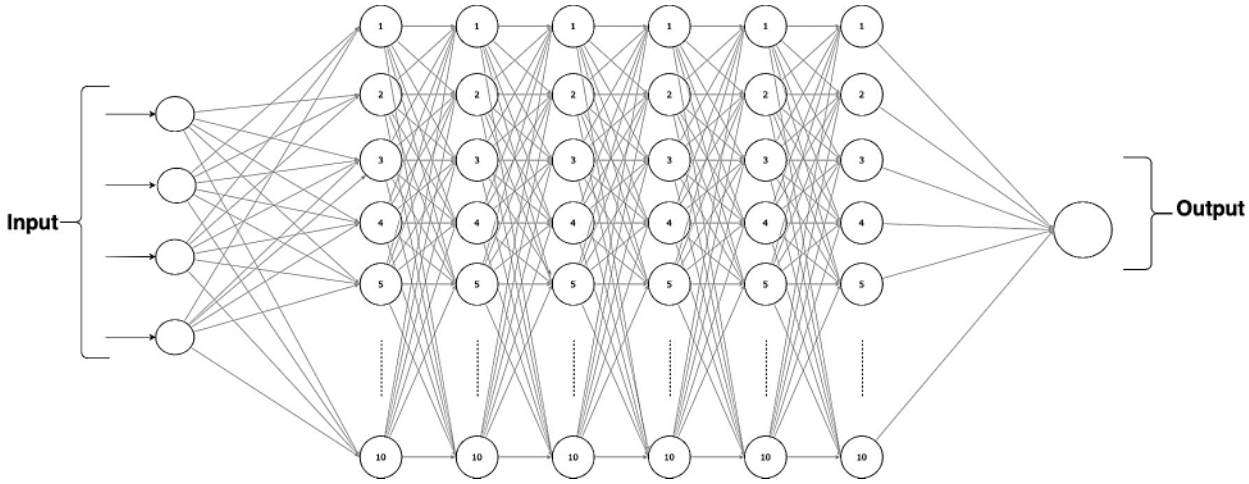

Figure 2: A systemic model of a Deep Extreme Learning Machine (DELM) [55]

Here $\mathfrak{q}_j$ and $\mathring{a}_j$ are learning variables, $ß_j$ is *jth* output node weight and $ç: § \to §$ is the activation function.

A perfect relation of several secret layers feed-forward neural network with reduced error demonstrates that with distinct intervals $\mathfrak{q}_j$ and a_j there occur $ß_j$ such that;

$$\mathrm{f}_i = \sum_{j=1}^{n} ß_j ç(\mathbf{p}_j \ni_{\mathrm{i}} + \mathring{a}_j) \quad i \in [1, Y] \tag{2}$$

Which can be represented as

$$\hat{U}ß = \mathbf{F} \tag{3}$$

where,

$$\hat{U} = \begin{bmatrix} ç(\mathfrak{q}_1 \ni_1 + \mathring{a}_1) & & ç(\mathfrak{q}_{\boldsymbol{n}} \ni_1 + \mathring{a}_n) \\ \vdots & \cdots & \vdots \\ \vdots & & \vdots \\ ç(\mathfrak{q}_1 \ni_N + \mathring{a}_1) & & ç(\mathfrak{q}_{\boldsymbol{n}} \ni_N + \mathring{a}_n) \end{bmatrix} \tag{4}$$

And

$$ß = (ß_1^T \ldots ß_n^T)^T, \mathbf{F} = (\mathrm{f}_1^T \ldots \mathrm{f}_Y^T)^T \tag{5}$$

When the number of observations above hidden layer neurons, the output value weights can be approximated by utilizing the method below

$$ß = \hat{U}^{-1}\mathbf{F} \tag{6}$$

And $\hat{U}^{-1}$ is the inverse of $\hat{U}$ matrix. Real-Time Deep Extreme Learning Machine (RTS-DELM) is consequently, a computationally effective method of investigation.

Backpropagation includes weighting configurations, forward adjustments, backward error updates, and distinguishability upgrading. These functions are all used in designing the neural network;

$$W = \frac{1}{2}\sum_{j}(t_z - r_z)2 \tag{7}$$

where t_z and r_z represents the desired output & calculated output respectively. Eq. (7) specifies a backpropagation error, which is designed by dividing the square amount of the necessary result by 2. The correction is appropriate to compensate for the usual errors. The updated weight values are indicated in the output layer in Eq. (8).

$$\Delta \mathrm{M}_{x,z}^{l=6} \propto -\frac{\partial \mathrm{D}}{\partial \mathrm{M}^{l=6}} \tag{8}$$

where x and z represent the number of neurons and output level respectively. The technique to enhance the weight and bias among the outcome and the hidden layer is illustrated in Eq. (9).

$$M_{x,z}^{l=6}(t) = M_{x,z}^{l=6}(t) + \lambda \Delta M_{x,z}^{l=6} \tag{9}$$

Eq. (10) displays how updating the weight and bias between the input and the hidden layer.

$$M_{x,n}^{l}(t) = M_{x,n}^{l}(t+1) + \lambda \Delta M_{x,z}^{l} \tag{10}$$

5 Results and Discussion

In this article, the Real-Time Deep Extreme Learning Machine (RTS-DELM) approach was implemented to the fused data [48,53]. The results were arbitrarily allocated to either the training collection (80% of the data means 118813 records) or the test/validation set (20% of the data means 29703 records). The information has been analyzed in anticipation of its planned use to assure that there are no mistakes. Real-Time Deep Extreme Learning Machine (RTS-DELM) sought to determine whether their devices had been infected by ransomware and cyber threats. We then analyzed a variety of neurons, including the stimulation of secret layers, different forms of active functions. In this experimental testing, we can evaluate the output of Real-Time Deep Extreme Learning Machine (RTS-DELM) to see if this approach is efficient. To estimate the performance of the Real-Time Deep Extreme Learning Machine (RTS-DELM) algorithm, we have employed numerous statistical measurements explaining the output in Eqs. (11) & (12).

$$\text{Miss rate} = \frac{\sum_{b=0}^{1}(F_b/V_{z\neq b})}{\sum_{b=0}^{1}(T_b)} \quad \text{Where, } z = 0, 1 \tag{11}$$

$$\text{Accuracy} = \frac{\sum_{b=0}^{1}(F_b/V_b)}{\sum_{b=0}^{1}(F_b)} \tag{12}$$

In Eqs. (11) and (12), F & V symbolizes the predictive output of WIoSNs and the actual output respectively. F_0 & V_0 represents that the forecast outcome is normal that no attack is detected in the real output. F_1 & V_1 signifies the malicious activity is detected in estimated output and actual output respectively. F_b/V_b symbolizes predictive and actual results are similar. Similarly, $F_b/V_{z\neq b}$ symbolizes error, in which predictive and actual results are changing.

Results of all datasets are extracted by each of the following training functions: Tab. 1 exhibited the suggested Real-Time Deep Extreme Learning Machine (RTS-DELM) based wireless sensor networks framework for prediction of intrusion detection during training level. Total 118813 records are utilized throughout the training which is then split into 61642, 57171 records of normal and attack correspondingly. It is witnessed that 59819 attack records of normal groups, having no real attack, are correctly forecasted by forecasting algorithm and 1823 attack records are inaccurately forecasted by this process. Comparably, a total of 58630 records is acquired in the circumstance of attack establish, in which 55240 records are accurately forecasted as an attack establish and 1931 records are inaccurately forecasted as a normal establish while attack exists there.

Table 1: Training of the Real-Time Deep Extreme Learning Machine (RTS-DELM) based decentralized wireless sensor networked device architecture for the estimation of intrusion with the fused dataset

Proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) based Wireless Sensor Networks (WSNs) framework			
(80% of data used during training)			
Total no. of records (N = 118813)		Outcome (Output) (F0, F1)	
Input	Predictable outcome (V0, V1)	F0 (Normal)	F1 (Attack)
	V0 = 61642 Normal	59819	1823
	V1 = 57171 Attack	1931	55240

Tab. 2 exhibited the suggested Real-Time Deep Extreme Learning Machine (RTS-DELM) based wireless sensor networks framework for prediction of intrusion detection during validation level. Total 29703 records are utilized throughout the training which is then split into 15411, 14292 records of normal and attack correspondingly. It is seen that 14569 records of normal class mean in which no attack discovered are accurately forecasted and 842 records are inaccurately forecasted as an attack establish while there is no actual attack. In the situation of assault, of the 14292 records obtained, 13227 were correctly forecasted as an invasion establishment, while 1065 were misleadingly forecasted as a regular establish while the attack occurred.

Tab. 3 exhibited the suggested Real-Time Deep Extreme Learning Machine (RTS-DELM) based wireless sensor networks framework assessment in the mean of accuracy and miss rate throughout training and validation level. It demonstrated that the suggested RTS-DELM based wireless sensor networks system during training gives 96.84% and 3.16% accuracy and miss rate collectively. And during validation, the proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) based wireless sensor networks system gives 93.58% and 6.42% accuracy and miss rate collectively.

Table 2: Validation of the Real-Time Deep Extreme Learning Machine (RTS-DELM) based decentralized wireless sensor networked device architecture for the estimation of intrusion with the fused dataset

Proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) based WIoSNs framework			
(20% of data used during validation)			
Total no. of records (N = 29703)		Outcome (Output) (F0, F1)	
Input	Predictable outcome (V0, V1)	F0 (Normal)	F1 (Attack)
	V0 = 15411 Normal	14569	842
	V1 = 14292 Attack	1065	13227

Table 3: Performance evaluation of proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) based decentralized wireless sensor networked device architecture for the estimation of intrusion with fused dataset during validation and training

	Accuracy	Miss rate	Sensitivty	Specificty
Training	96.22%	3.16%	0.97	0.96
Validation	92.73%	6.42%	0.94	0.92

We compared the reliability of our method with the other published algorithms. As seen in Tab. 4, with a smaller error rate, the proposed framework attains extensively enhanced accuracy. The suggested Real-Time Deep Extreme Learning Machine (RTS-DELM) framework is better as compare to other algorithms in terms of accuracy such as Support vector machine (SVM) [48], self-organization map [49], artificial neural network-based intrusion detection system [50], discriminative multinomial naïve bayes [51] and Generative adversarial networks (GANs) [52]. The increased precision attained by the proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) method attains improved efficiency on the fused dataset compared to the NSL-KDD dataset. In comparison to other deep learning methods, the precision of the SVM [48] is much less. In [51], using a mixture of discriminative multinomial naïve bayes and random estimates, the researchers obtained a score of approximately 80%. In [49], the authors suggested Self-Organization Map and, in this method, the investigators achieved 75.5% accuracy. In [50], the authors suggested an artificial neural network-based intrusion detection system, and, in this method, the researchers achieved 81.2% precision. In [52], the researchers proposed GANs and in this method, the investigators achieved 86.5% precision. The Real-Time Deep Extreme Learning Machine (RTS-DELM) system has an accuracy of 93.58 percent which is higher than previous attempts showing its effectiveness. The proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) paradigm offers a substantially improved value than other strategies. The suggested Real-Time Deep Extreme Learning Machine (RTS-DELM) paradigm provides a plausible answer to the aforementioned dilemma.

Table 4: Comparison results of the proposed data fusion technique of wireless sensor networks based on real-time sequential deep extreme learning machine with literature

Method	Accuracy rate
Support Vector Machine [48]	69.5%
SOM [49]	75.5%
Artificial Neural Network-based Intrusion Detection System [50]	81.2%
DMNB [51]	81.5%
Generative Adversarial Networks [52]	86.5%
Real-Time Deep Extreme Learning Machine (RTS-DELM) with Data Fusion Approach (Proposed)	93.58%

6 Conclusions

A system of fused data for wireless network intrusion detection has been developed to improve prediction accuracy. Different methodological techniques have been used to evaluate the feasibility of this specific proposal. These experiments indicate that the Real-Time Deep Extreme Learning Machine (RTS-DELM) process is far more successful than other approaches. The proposed Real-Time Deep Extreme Learning Machine (RTS-DELM) method is leading to its effectiveness. The suggested application demonstrated an accuracy level of 96.84% and 93.58% on testing. Additionally, it is known that using a simplified algorithm is less costly and faster to execute. In the presented analysis, ELM is used to outline the benefits of machine learning and a deep network. We are confident of the initial outcomes and intend to broaden this study in the future by testing further datasets. The limitation of the proposed system is the computational complexity due to the increasing number of hidden layers. Future research shall seek to more precisely define and measure the parameters. The learning algorithm will be retrained more regularly to boost the efficiency of different configurations.

Acknowledgement: We thank our families and colleagues who provided us with moral support.

Funding Statement: The author(s) received no specific funding for this study.

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

References

[1] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli *et al.,* "Understanding smart cities: An integrative framework," in *45th Hawaii Int. Conf. on System Science*, Maui, Hawaii USA, pp. 2289–2297, 2012.

[2] A. Fatima, M. A. Khan, S. Abbas, M. Waqas, L. Anum *et al.*, "Evaluation of planet factors of smart city through multi-layer fuzzy logic," *Isc International Journal of Information Security*, vol. 11, no. 3, pp. 51–58, 2019.

[3] A. Atta, S. Abbas, M. A. Khan, G. Ahmed and U. Farooq, "An adaptive approach: Smart traffic congestion control system," *Journal of King Saud University-Computer & Information Sciences*, vol. 32, no. 9, pp. 1012–1019, 2020.

[4] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak and R. Morris, "Smarter cities and their innovation challenges," *Computer*, vol. 44, no. 6, pp. 32–39, 2011.
[5] M. Z. Hasan, H. A. Rizzo and F. A. Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1424–1456, 2017.
[6] A. Mestres, A. R. Natal, J. Carner, P. B. Ros, E. Alarcon *et al.,* "Knowledge-defined networking," *Acm Sigcomm Computer Communication Review*, vol. 47, no. 33, pp. 2–10, 2017.
[7] S. Pudlewski, A. Prasanna and T. Melodia, "Compressed-sensing-enabled video streaming for wireless multimedia sensor networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 6, pp. 1060–1072, 2012.
[8] S. M. Aziz and D. M. Pham, "Energy-efficient image transmission in wireless multimedia sensor networks," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1084–1087, 2013.
[9] T. Wang, L. Qiu, A. K. Sangaiah, A. Liu, M. Z. A. Bhuiyan *et al.,* "Edge-computing-based trustworthy data collection model in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4218–4227, 2020.
[10] M. Dohler, I. Vilajosana, X. Vilajosana and J. Llosa, "Smart cities: An action plan," in *Proc. of Barcelona Smart Cities Congress*, Barcelona, Spain, pp. 1–6, 2011.
[11] R. Khare and P. Shrivasta, "Data mining for the internet of things," in *Exploring the Convergence of Big Data & the Internet of Things*, Chicago, pp. 181–191, 2018.
[12] H. Anandakumar and K. Umamaheswari, "Supervised machine learning techniques in cognitive radio networks during cooperative spectrum handovers," *Cluster Computing*, vol. 20, no. 2, pp. 1505–1515, 2017.
[13] K. M. Thilina, K. W. Choi, N. Saquib and E. Hossain, "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2209–2221, 2013.
[14] 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, 2012.
[15] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani *et al.,* "Smart cities of the future," *European Physical Journal Special Topics*, vol. 214, no. 1, pp. 481–518, 2012.
[16] M. Wang, Y. Cui, X. Wang, S. Xiao and J. Jiang, "Machine learning for networking: Workflow, advances and opportunities," *IEEE Network*, vol. 32, no. 2, pp. 92–99, 2018.
[17] M. Usama, J. Qadir, A. Raza, H. Arif, K. Yau *et al.,* "Unsupervised machine learning for networking: Techniques, applications and research challenges," *IEEE Access*, vol. 7, pp. 65579–65615, 2019.
[18] G. Xu, Y. Mu and J. Liu, "Inclusion of artificial intelligence in communication networks and services," *Itu Journal: Ict Discoveries*, vol. 1, no. 1, pp. 1–6, 2017.
[19] M. Ahmed, A. N. Mahmood and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network & Computer Applications*, vol. 60, pp. 19–31, 2016.
[20] T. T. Nguyen and G. Armitage, "Timely and continuous machine learning-based classification for interactive IP traffic," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1880–1894, 2012.
[21] 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.
[22] 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.
[23] 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*, no. 3, pp. 1379–1391, 2015.
[24] L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[25] 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. 19, no. 4, pp. 2392–2431, 2017.
[26] 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.
[27] 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. 2017, pp. 1–8, 2017.
[28] X. Zhou, M. Sun, G. Y. Li and B. H. Juang, "Machine learning and cognitive technology for intelligent wireless networks," *Information Theory*, vol. 17, pp. 1–53, 2017.
[29] 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. 2017, pp. 1–10, 2017.
[30] W. Peng, C. Li, G. Zhang and J. Yi, "Interval type-2 fuzzy logic based transmission power allocation strategy for lifetime maximization of WSNs," *Engineering Applications of Artificial Intelligence*, vol. 87, pp. 103269–103282, 2020.
[31] Q. Yan, W. Peng and G. Zhang, "Optimal energy consumption tasks scheduling strategy for multi-radio WSNs," *Sensors*, vol. 20, no. 3, pp. 881–896, 2020.
[32] Q. Wu, G. Ding, Y. Xu, S. Feng, Z. Du *et al.,* "Cognitive internet of things: A new paradigm beyond connection," *IEEE Internet of Things*, vol. 1, no. 2, pp. 129–143, 2014.
[33] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos *et al.,* "Enabling smart cities through a cognitive management framework for the internet of things," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 102–111, 2013.
[34] S. Eckert and S. Kohler, "Urbanization and health in developing countries: A systematic review," *World Health Popul*, vol. 15, no. 1, pp. 7–20, 2014.
[35] I. Zubizarreta, A. Seravalli and S. Arrizabalaga, "Smart city concept: What it is and what it should be," *Journal of Urban Planning & Development*, vol. 142, no. 1, pp. 04015005–04015017, 2016.
[36] R. P. Dameri, "Defining an evaluation framework for digital cities implementation," in *Int. Conf. on Information Society*, London, pp. 466–470, 2012.
[37] X. Xiaojiang, W. Jianli and L. Mingdong, "Services and key technologies of the internet of things," *Zte Communications*, vol. 8, no. 2, pp. 26–29, 2020.
[38] R. Kitchin, "The real-time city? big data and smart urbanism," *Geo Journal*, vol. 79, no. 1, pp. 1–14, 2014.
[39] F. Francois and E. Gelenbe, "Optimizing secure SDN-enabled inter-data center overlay networks through cognitive routing," in *IEEE 24th Int. Symp. on Modeling, Analysis & Simulation of Computer & Telecommunication Systems*, London, pp. 283–288, 2016.
[40] E. R. Neto, J. R. G. D. Rosa, M. A. F. Casaroli, I. F. D. Costa, A. M. Alberti *et al.,* "Implementation of an optical-wireless network with spectrum sensing and dynamic resource allocation using optically controlled reconfigurable antennas optically controlled reconfigurable antennas," *International Journal of Antennas & Propagation*, vol. 2014, pp. 1–11, 2014.
[41] B. Shan, H. Ji and Y. Li, "Centralized compressed sensing with structurally random matrix in cognitive WLAN over fiber," in *IEEE Wireless Communications & Networking Conf.*, Shanghai, China, pp. 106–111, 2013.
[42] Y. Li, H. Ji, X. Li and V. Leung, "Dynamic channel selection with reinforcement learning for cognitive WLAN over fiber," *International Journal of Communication Systems*, vol. 25, no. 8, pp. 1077–1090, 2012.
[43] R. Urgaonkar and M. J. Neely, "Opportunistic cooperation in cognitive femtocell networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 607–616, 2012.
[44] S. Al-Rubaye, A. A. Dulaimi and J. Cosmas, "Cognitive femtocell," *IEEE Vehicular Technology Magazine*, vol. 6, no. 1, pp. 44–51, 2011.
[45] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-defined networking and distributed denial of service attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2015.

[46] B. Yuan, D. Zou, S. Yu, H. Jin, W. Qiang *et al.,* "Defending against flow table overloading attack in software-defined networks," *IEEE Transactions on Services Computing*, vol. 12, no. 2, pp. 231–246, 2016.

[47] S. Dev, B. Wen, Y. H. Lee and S. Winkler, "Ground-based image analysis: A tutorial on machine-learning techniques and applications," *IEEE Geoscience & Remote Sensing Magazine*, vol. 4, no. 2, pp. 79–93, 2016.

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

[49] L. M. Ibrahim, D. T. Basheer and M. S. Mahmod, "A comparison study for intrusion database (kdd99, Nsl-kdd) based on self-organization map artificial neural network," *Journal of Engineering Science & Technology*, vol. 8, no. 1, pp. 107–119, 2013.

[50] B. Ingre and A. B. Yadav, "Performance analysis of NSL-kDD dataset using ANN," in *IEEE Int. Conf. on Signal Processing & Communication Engineering Systems*, Guntur, India, pp. 92–96, 2015.

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

[52] R. Alshinina and K. Elleithy, "A highly accurate machine learning approach for developing wireless sensor network middleware," in *Wireless Telecommunications Symp.*, Phoenix, AZ, United States, pp. 1–7, 2018.

[53] M. H. Zaib, (2020, January) Kaggle, 2019. [Online]. Available: https://www.kaggle.com/hassan06/nslkdd.

[54] A. Haider, M. A. Khan, A. Rehman, M. U. Rahman and H. S. Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1785–1798, 2020.

[55] 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, no. 1, pp. 39982–39997, 2020.

[56] 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 & Smart Environments*, vol. 12, no. 2, pp. 125–138, 2020.

[57] M. A. Khan, S. Abbas, K. M. Khan, M. A. Ghamdi 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.

[58] J. Cheng, Z. Duan and Y. Xiong, "QAPSO-Bp algorithm and its application in vibration fault diagnosis for a hydroelectric generating unit," *Journal of Vibration & Shock*, vol. 34, no. 23, pp. 177–181, 2015.

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