ZANCO Journal of Pure and Applied Sciences

TYPE Original article
DOI http://dx.doi.org/10.21271/ZJPAS.36.6.14

OPEN ACCESS

*Corresponding author
Ahmed Abdulfatah Abdlrazaq
ahmed.abdulfatah @su.edu.krd

Contextual Deep Semantic Feature Driven Multi-Types Network Intrusion Detection System for IoT-Edge Networks

Shaho Ismael Hassen[1] ,Ahmed Abdulfatah Abdlrazaq[2]

1Department of Petro-Chemical Engineering, College of Engineering
Salahaddin University-Erbil, Erbil, Kurdistan Region, Iraq
2 ICT Center,Salahaddin University-Erbil,Erbil, Kurdistan Region, Iraq

RECEIVED :03 /05/2024
ACCEPTED :25/11/ 2024
PUBLISHED :31/12/ 2024

KEYWORDS:
Edge-IoT Network, Network Intrusion Detection, Semantic Contextual Feature Learning, Cascaded Recurrent Networks, Bi-LSTM.

ABSTRACT

Recent years have witnessed an exponential rise in wireless networks and allied interoperable distributed computing frameworks, where the different sensory units transfer real-world event data to the network analyzer for run-time decisions. There exists an array of applications employing edge- internet of things (Edge-IoT) where the edge nodes collect local data to perform real-time decisions. However, the at-hand edge-IoT systems being decentralized, infrastructure-less, and dynamic remain vulnerable to man-in-the-middle attacks, intrusion, denial of service attacks, etc. Though in the past, numerous efforts were made towards intrusion detection in IoT networks, the major approaches focused merely on standalone intrusion detection, and therefore their scalability towards multiple attack detection remains unaddressed. On the contrary, applying a unit intrusion detection system for each type of attack can impose resource exhaustion and delay. Recently authors have used deep learning methods like convolutional neural network (CNN), and long- and short-term memory (LSTM) to perform learning-based intrusion detection. However, being reliant on merely local features its reliability remains suspicious. Such methods ignore long-term dependency problems that limit their efficacy in intrusion detection in temporal Edge-IoT network traffic. With this motivation, in this paper, a contextual deep semantic feature-driven multi-type intrusion detection model (CDS-MNIDS) is proposed for Edge-IoT networks. The proposed CDS-MNIDS model at first performs network traffic segmentation from the temporal network traces obtained from the network gateway. Subsequently, the node's dynamic features including the node's address, packet size, transmission behavior, etc., are processed for Word2Vec encoding, followed by a cascaded deep network-based learning and prediction. The CDS-MNIDS model embodied a cascaded deep network encompassing LSTM and bidirectional LSTM networks, where the first extracted local features. At the same time, the latter obtained contextual features from the input local feature vector. The extracted local and contextual features were projected to the global average pooling layer followed by the fully connected layer that in conjunction with the Softmax layer performed multi-class classification.
The simulation results demonstrated a multi-type intrusion detection accuracy of 99.81%, with a precision of 98.81%, a recall of 98.48%, and an F-measure of 0.985. These values are superior compared to those of other existing intrusion detection models.

1.Introduction

In the last few years, the wireless communication networks, advanced software computing techniques, interoperable distributed computing infrastructures have gained widespread attention to serve scalable and time-efficient monitoring and control services. The proliferation of inexpensive hardware sensors has expanded the scope of the aforementioned technologies to encompass a wide range of applications in e-Healthcare, industrial monitoring and control, surveillance systems, smart factory operations, defense, and commercial communication systems (Jiang et al., 2020b). To cope up such application environments, the aforesaid technologies have evolved decisively where the advanced technologies such as the internet-of-things (IoT), machine-to-machine (M2M) communication systems, edge-computing etc. have gained widespread attention. The other technological evolutions such as the mobile-wireless sensor networks (MWSN), mobile ad-hoc networks (MANET), vehicular ad-hoc networks (VANET) (Li et al., 2022). too have gained decisive attention across industries globally. The high-pace up-surging significances have motivated industries and civic management bodies to exploit aforesaid communication networks to serve scalable real-time services. Edge-based IoT systems, where sensor nodes or edge nodes are installed to gather data and interact with the network analyzer or control nodes, can be dynamic, making identifying abnormalities or attack circumstances problematic (Farivar et al., 2020). The dynamic nature of such nodes often broadens the horizon for intruders to gain network access either by mimicking a genuine or authenticated node or by intruding network infrastructure due to poorly coupled security framework (Liao et al., 2020, Vinayakumar et al., 2020). Being decentralized and infrastructure-less network characteristics the likelihood of intrusion can't be ruled out, especially under uncertain network conditions, dynamic channels and aforesaid intrusion cases. To alleviate it, applying network intrusion detection systems seems to be an inevitable requirement. To cope up such demands, in the past a large number of efforts have been made where the authors have applied node parameters or its dynamic behavior such as packet delivery rate (PDR), link-loss, delay etc. to perform intrusion detection. For instance, the denial of service (DoS) and reply attacks are identified by means of assessing a node's timeliness in response, while eavesdropping is quantified due to the iterative retransmission demands. Thus, applying such node behaviors the nodes are classified as normal or abnormal. Additionally, the nodes static characteristics such as node ID, destination ID, packet size, packet length, topology too are applied to perform intrusion detection (Huang et al., 2020). However, almost major state-of-arts have exploited aforesaid node parameters to detect standalone kind of intrusion or network attack detection. It signifies that a network intrusion detection model designed based on delay information can merely be employed to detect DoS or replay attacks (Liu et al., 2020, Chen et al., 2019). The same can't be suitable to decide other attack types and therefore, a typical Edge-based IoT network which employs both dynamic network characteristics as well as a large number of interconnected cooperative or autonomous nodes for communication might demand multiple network security models to ensure network security and attack-resilience. Intrusion Detection Systems (IDS) act as vigilant guardians in the intricate realm of network security. These systems aim to identify and react to suspicious network traffic that suggests malicious activities. Experts have categorized IDS systems into two types: signature-based and anomaly-based. Yet, these tools have grown to tackle the tricky problems that come with today's network setups, including the Internet of Things (IoT) (Chen et al., 2019). Systems that use signatures rely on known patterns of attacks we've seen before, while those that look for anomalies spot oddities compared to what's seen. When it comes to the Internet of Things (IoT), with its mix of different gadgets and network layouts, many think it's key to use a blended approach. This method takes the best

parts of both ways of thinking to deal with and lower risks.

In real-world Edge-IoT networks a network might undergo different kinds of attack conditions, where the behavioral pattern or characteristics of a node (say, attacker node) might vary from another(S. Liu, 2020). In this case, merely applying single attack-specific feature towards scalable and multi-type attack detection can yield false positive or false negative performance (Chen et al., 2019). For instance, unlike blackhole attacks, the wormhole attack causes tunnelling of the data packets between two target locations by applying in-band as well as out-band channels. In this attack condition, two or multiple intruders create peer-tunnel architecture to bypass the target data. It often results into data-losses and complete transmission failure between intended source-destination node pair(s). Similar to the blackhole attack condition, in gray hole attack case the intruder can drop the packets randomly or with certain probability (Chen et al., 2019, Butun et al., 2020). Here, the attacker node can drop packets from a specific node while it can forward the packet to the other irrelevant node, thus disrupts entire communication network. Its ability to drop traffic specific packets like dropping all transmission control protocol (TCP) packets while transmitting user datagram protocol (UDP) packets degrades overall network reliability and performance(Huang et al., 2020, Liu et al., 2020) (Chen et al., 2019). In a sinkhole attack, a malicious (sinkhole) node advertises a best possible route to the BS which misguides its neighbors in order to use that route more frequently. The malicious node thus gets an opportunity to tamper with the data, damage the regular network operations or conduct other serious threats. Misdirection attack too routes the packets from its neighbors to other distant nodes, but not necessarily to its legitimate destination nodes. This produces a long delay in packet delivery and decreases throughput of the network (Butun et al., 2020, Khan et al., 2019, Elbahadır and Erdem, 2021). Unlike above stated attack conditions, in hello-flood attack a malicious node captures a sensor node and broadcasts hello massages, and declares itself as a neighbor node. Subsequently, it causes packet loss and hence perform degradation(Butun et al., 2020). The use of delay information is applied towards DoS attacks, while packet loss or packet delivery rate information is used to detect flooding attack(Chen et al., 2019, Butun et al., 2020). It signifies that in majority of the existing researches authors have employed different network parameters to detect the different attack type(Khan et al., 2019). In such undeniable network conditions, applying multiple parallel or sequential network intrusion detection systems within aforesaid Edge-IoT networks can cause significant resource exhaustion and therefore can limit the scalability and longevity of the network solution. Such classical approaches can also impact quality-of-service (QoS) aspects of the Edge-IoT networks, thus making it unsuitable for real-world communication demands(Elbahadır and Erdem, 2021) .

The above inferences clear indicate that to enable a resource-efficient, computationally efficient and reliable Edge-IoT communication there is the need of a multi-type intrusion detection framework, which could be able to detect the different attacks or intrusion without employing separate intrusion detection solutions. To meet QoS demands and allied multi-type intrusion detection, training a machine learning or artificial intelligence (AI) tool over the network behavior information can be of great significance. In this reference, in the past a number of efforts were made by learning node's behavior to perform intrusion detection. The classical approaches such as the convolutional neural networks (CNN) deep learning methods or long and short-term memory (LSTM) is A type of RNN for processing sequential data and methods were applied extensively to perform network intrusion detection; however, such methods are often criticized because of their inability to address long-term dependency, severe gradient vanishing and lack of contextual details to achieve reliable prediction. To address such issues developing a robust deep driven approach employing both local as well as

contextual details derived from the network dynamic information such as node identity information, medium access control (MAC) parameters, link-layer information, etc. can be of paramount significance. In other words, designing a robust deep learning framework which could exploit both local as well as global (say, contextual) features obtained from the nodes behavior can make learning more efficient to make reliable intrusion detection decision. Additionally, training a robust deep network with the node behavior or patterns representing the different attack types too can enable a cost-effective and scalable multi-type intrusion detection and classification system. Unfortunately, very few efforts have been made towards Ai-based multi-type intrusion detection in Edge-IoT network. Moreover, those efforts made towards network intrusion detection systems, especially by using deep learning networks have ignored aforesaid long-term dependency problems, lack of contextual details etc. that confine their suitability to meet real-world network demands. To alleviate such problems, there is the need of a robust deep network which could guarantee multi-type intrusion detection by addressing aforesaid computing challenges or limitations (i.e., long-term dependency problems, lack of contextual details, etc.). It can be considered as the key driving force behind this research.

The research is situated within the rapidly evolving landscape of IoT networks, characterized by the convergence of wireless communication, advanced computing, and low-cost sensors. This confluence of technologies has enabled a wide array of applications across diverse sectors, including healthcare, industry, surveillance, and defense. However, the decentralized and dynamic nature of IoT networks, coupled with the increasing sophistication of cyber threats, has necessitated robust security measures. The research focuses on the development of an intrusion detection system (IDS) specifically tailored for Edge-IoT environments. The primary objective is to address the limitations of existing IDS solutions in detecting multiple types of attacks simultaneously and efficiently.

In sync with aforesaid research gaps and allied motivations, This study presents the development of a new effective CDS-MNIDS for Edge-IoT networks, addressing the research gaps and reasons mentioned before. The CDS-MNIDS security framework was designed in such manner that it extracts and trains over sufficiently large semantic features obtained from the temporal network logs to detect and predict multiple types attack conditions. It targeted to address at hand challenge of gradient vanishing and long-term dependency, which is quite often ignored by major at hand network intrusion detection systems. In this reference, this paper proposes cascaded recurrent deep network which could exploit both local as well as contextual (global) features from the network traffic data to perform multi-type intrusion detection.

The other sections of this paper are divided as follows. Section II discusses the related work, while the research questions are given in Section III. The overall proposed model and its implementation followed by conclusion are given in Section IV and Section V, respectively. The references used are given at the end of the manuscript.

2.Related Work

This section discusses some of the recent AI driven intrusion detection systems, where machine learning and deep learning methods are applied to detect intrusion of the specific type(s).

(Umamaheshwari et al., 2021)applied support vector machine (SVM) algorithm that exhibited an accuracy of over 99% with NSL-KDD network dataset. To improve time and learning efficiency, (Wang et al., 2017) applied principal component analysis (PCA) and genetic algorithm (GA) heuristic methods to retain most decisive features, which were later learnt by using SVM to perform intrusion detection. Yet, it achieved the highest accuracy of 96%. (Kuang et al., 2014) amalgamated particle swarm optimization (PSO) heuristic with SVM classifier towards intrusion detection. The simulation over

KDD99 dataset resulted the highest accuracy of 92.90%, putting question on its efficacy (Umamaheshwari et al., 2021, Wang et al., 2017). (Aburomman and Ibne Reaz, 2016) proposed hypergraph-based GA (HG-GA) to select most representative samples, while was later applied for SVM-based classification. This method exhibited the intrusion detection accuracy of 97.14% with NSL-KDD dataset. (Gauthama Raman et al., 2017) applied decision tree and SVM algorithms over KDD-CUP99 dataset where the highest accuracy of 89.02% was yielded by the SVM classifier. (Teng et al., 2018) applied random forest ensemble classifier on NSL-KDD dataset that exhibited the highest accuracy of 99.6%. (Farnaaz and Jabbar, 2016) on the other hand got 98.3% prediction accuracy with KDD99 dataset with the RF ensemble that put question on the generalizability of the previous RF-based works. (Elbasiony et al., 2013) developed an optimal allocation based least square SVM (OA-LS-SVM) method for network intrusion detection. (Kabir et al., 2018) applied k-NN classifier, which could achieve the highest intrusion prediction accuracy of 94%. (Li et al., 2018) applied Naïve Bayes (NB), SVM and RF algorithms for DoS intrusion detection in wireless sensor network. (Abdullah et al., 2018) applied neural network Bayesian Net-GR algorithm where the Gain Ratio (GR) was applied to perform feature selection followed by intrusion detection decisions. (KumarShrivas and Kumar Dewangan, 2014) applied self-taught learning (STL) based on deep network to perform intrusion detection. They applied CNN to perform feature extraction, which was applied by STL to perform feature selection followed by SVM for two-class classification. In (Al-Qatf et al., 2018) and (Lee et al., 2013), PCA and linear discriminant analysis (LDA) feature selection methods were applied that in conjunction with the Ant Lion optimization heuristic yielded sufficiently large feature vector for NN-based DDoS prediction. (Jaber et al., 2018) employed k-NN assisted clustering followed by the extreme learning machine (ELM) method to perform intrusion detection. (Latah and Toker, 2020) used NB and AdaBoost methods for network intrusion detection, where AdaBoost resulted intrusion prediction accuracy of almost 92%. Despite exhaustive approach where (Wahba et al., 2015) designed an ensemble learning method embodying DT, RF, k-NN and deep NN as base classifier to perform intrusion detection in NSL-KDD dataset. The simulation results confirmed superiority of the ensemble learning method that exhibited accuracy of 85.2%, which was higher than the DT classifier (accuracy 84.2%). Neural network methods were applied in (Gao et al., 2019, Beghdad, 2008, Song et al., 2006, Tran et al., 2012, Abuadlla et al., 2014) as well; yet, these methods yielded low prediction accuracy. A few clustering based approaches like the optimum-path forest clustering (Jadidi et al., 2013), sub-space and density-based clustering methods (Lakhina et al., 2005) were proposed towards network intrusion detection. Yet, these methods underwent reduced intrusion prediction accuracy and lack of generalizability over uncertain attack types. (Casas et al., 2011) applied a total of 39 network parameters which were trained over the RF ensemble algorithm to perform network intrusion detection. Yet, the accuracy of 90% puts question on its generalizability (Stevanovic and Pedersen, 2014). Despite their claim to have higher intrusion detection accuracy with the ELM algorithms; the limitations to have single-type intrusion detection limit their scalability. Marir et al. (Ahmad et al., 2018) used convolutional neural network for feature extraction followed by SVM learning for intrusion prediction. (Marir et al., 2018) used auto-encoder feature leaning with neural network for network intrusion detection. (Mirsky et al., 2018) applied a conditional variational autoencoder (CVAE) with LSTM recurrent neural networks (LSTMRNNs) for network intrusion detection (Lopez-Martin et al., 2017). Yet, they failed to address the issues of long-term dependency, gradient vanishing and lack of contextual information that can have decisive impact on the prediction accuracy. (Jiang et al., 2020a) applied semantic features for transfer-learning-based intrusion detection. While semantic features offer significant advantages for transfer-learning-based intrusion

detection systems, careful consideration must be given to their implementation and potential drawbacks. Balancing these strengths and weaknesses is crucial for developing effective and reliable intrusion detection mechanisms.

3.Research Questions

In sync with the overall research intends and allied scopes, this paper formulates certain questions whose justifiable answers put foundation for a robust and efficient multi-type network intrusion detection system for Edge-IoT systems. These questions are:

RQ1 *The amalgamation of static and dynamic network pattern-driven semantic features with a cascaded LSTM Bi-LSTM , an LSTM that processes data in both forward and backward directions network can effectively enhance multi-type network intrusion detection in Edge-IoT environments, as can the strategic integration of static and dynamic node behavior information.*

RQ2*: Can the use of Word2Vec semantic features obtained from the nodes' behaviour pattern enable better feature extraction and learning to yield accurate and reliable intrusion detection system for Edge-IoT systems?*

RQ3*: Can the use of cascaded recurrent neural networks be encompassing LSTM and Bi-LSTM deep networks in conjunction with global average pooling layer and fully connected layer yield reliable multi-type network intrusion detection and classification for scalable Edge-IoT network security?*

Thus, this research aims to achieve justifiable answers for these questions that eventually can put foundation for a robust Edge-IoT network security solution.

4.System Model

The overall proposed model encompasses the following sequential steps:

1. *Network Data Acquisition and Pre-processing*
2. *Static-o-Dynamic (Traffic) Parameter Segmentation*
3. *Word2Vec Semantic Feature Mapping*
4. *Cascaded Deep Network for Feature Extraction and Learning, and*
5. *Performance Characterization.*

The subsequent sections offer a comprehensive discussion of the proposed model in (Fig. 1).

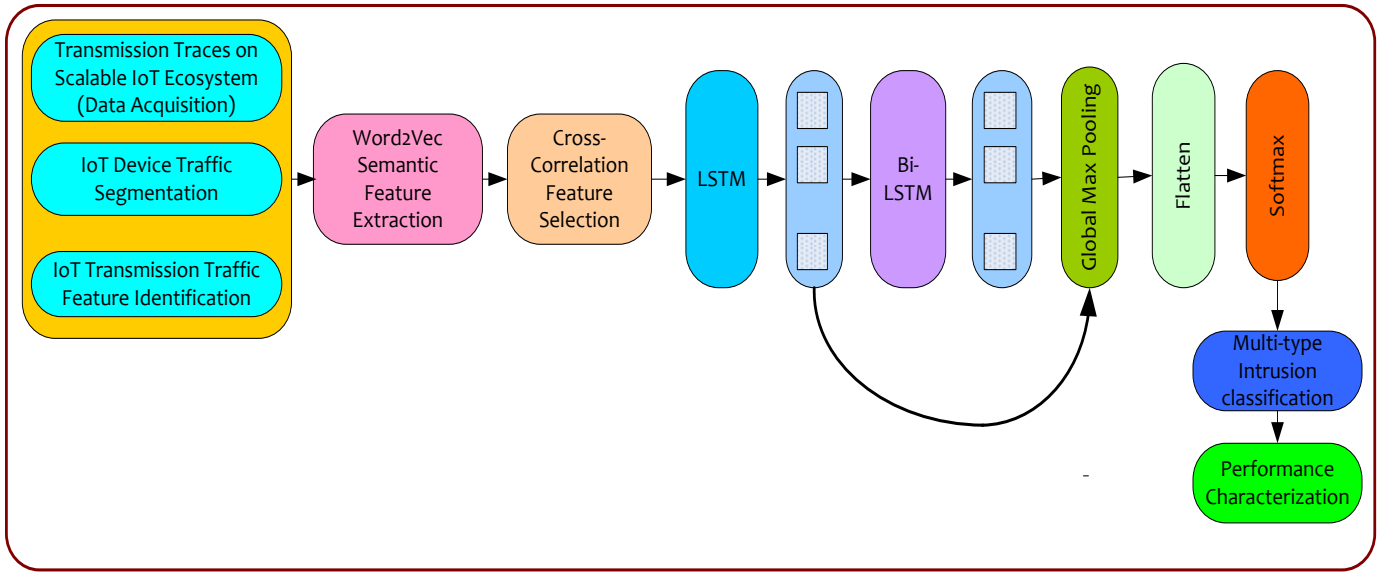

Fig. 1: Proposed Method

The sequential implementation detail is given as follows:

A. Network Data Acquisition and Pre-Processing

To achieve our research goal of detecting various types of intrusions or network attacks, we collected IoT network traces from numerous nodes operating both autonomously and collaboratively. More specifically, in this work, a benchmark dataset embodying inter IoT (edge) node communication patterns over a large number of deployed sensors was obtained. We collected the IoT communication data traffic from the University of New South Walles (UNSW), which is normally known as UNSW NB15 dataset. Recalling the fact that the proposed research focuses on designing a robust multi-type intrusion detection solution, UNSW NB15 dataset was considered as it embodies intrusion traces pertaining to the wormhole attacks, DoS attack, Fuzzers etc. The dataset exhibits significant class imbalance, with normal records constituting about 87% of the total data. In contrast, the combined attack classes make up only 13%, leading to challenges in training models that can accurately detect less frequent attacks. This imbalance can increase the false positive rate and decrease detection accuracy for underrepresented classes.

In UNSW data preparation, the cyber security experts representing the Australian Centre for Cyber Security (ACCS) were involved who deployed the network and allied data generation model at the University of New South Wales (Australia) in 2015, where executing the traffic and allied sensor communication over 1000s of hours, the final network traces were obtained. In the considered data environment, there are a large number of sensor nodes (say, IoT sensors or edge nodes) deployed across the network area. The UNSW-NB15 dataset houses the communication traffic between these nodes where the gateway node monitors inter-node communication and creates log for further analysis. In sync with the demand of a scalable network condition for deep learning methods, over both normal as well as intrusion transmission or traffic cases, the UNSW NB15 dataset applied multiple servers where the traffic injection tool was applied to injects traffic instances amongst the different sensor nodes. In addition to the simulated data traffic, this specific dataset has applied IXIA Perfect Storm tool that generates sufficient traffic with both normal as well as intrusion cases (say, traffic) for further intrusion detection and classification. Let, N_1, N_2 and $N_n$and N_a, N_b and N_n be the edge devices or sensors deployed across the network, while S_1, S_2 and S_n be the servers generating network traffic amongst aforesaid devices or nodes. The inter-node communication traces are subsequently processed by $TCPDump$ tool that enables node's specific pattern segmentation. It also enables traffic segmentation and allied feature identification, which is later used to perform learning-based (network intrusion) prediction. In this work, the $TCPDump$ tool was applied to collect device's address ($IP\_Address$, MAC Addresses, source and destination addresses etc.), transmission $Protocol$ used, type of the data, data size, transmission period (delay information), packet received information, packet size etc.

A sippet of the dataset considered in this work and allied statistical details is given in Table I. The overall considered dataset embodies network traffics representing normal traffics as well as six different kinds of intrusion pattern or traffic instance. The use of two distinct servers in conjunction with the IXIA traffic generation tools provided sufficiently large data traces to improve learning and prediction accuracy. It also helped to annotate traffic types, which made deep learning easier to achieve higher accuracy. The total dataset considered had the network transaction traces counting 2 million. The overall data was split into two parts; training and testing data, where we considered 60% data for training while remaining 40% was applied for testing. As stated earlier, we considered seven different kinds of data cases including six intrusion patterns and one normal traffic traces. The considered dataset embodied normal traces, Fuzzers, DoS attacks, Wormhole attacks, Shell-code attacks, and Reconnaissance attacks. In real world scenario there can be the probability that a sensor can keep transmitting traffic with no events and even certain sensors or edge devices

can transmit rarely to update interval-based assessment. Such conditions can give rise to the data imbalance and therefore, we performed network segmentation which helped to identify the active period detail about each and every deployed (active) node. In this reference, the node specific details such as the node addresses (i.e., transmitter and receiver $IP\_Address$), transmission protocol, data traffic type, data length, transmission period (i.e., delay), packet received information, packet size etc. were obtained.

Table I: UNSW-NB15 dataset

Class	Description	Training	Testing
Normal	Normal connection records	56000	37000
Fuzzers	Attacks related to spams, HTML files penetrations, and spam and port scams	18184	6062
DoS	Intruder intends to deplete the resources and make network down, thereby making entire system and resource inaccessible	12264	4089
Generic	Attacks are related to the block-cipher	14000	18871
Reconnaissance	A target system is observed by an attacker to gather information for vulnerability	10491	3496
Shell code	It is a small part of program learned as payload used in exploitation of a software	1133	378
Worms	They replicate themselves and get distributed across the system to get access to the resources as well as operating computer network(s).	130	44

B. Static-o-Dynamic (Traffic) Parameter Segmentation

In the targeted Edge-IoT networks there can be a large number of resource constrained edge devices or IoT devices interfaced through the wireless transmission channels. Once transmission initiates the connected nodes or edge devices start transmitting the real-time data, and continues transmitting data traces depicting node information, data type, traffic size, frame size, delay information, device types, source and destination ID, roles, configuration with gateway or collaborated nodes, service types etc. In real-world transmission, the edge devices can perform peer-communication directly or via gateway or server node(s). On the other hand, the different edge devices or IoT sensors can use the different routing protocol; though, the major at hand solutions apply TCP/IP protocols to achieve transmission. Thus, the complete network traffic can be defined as a time-series data possessing the different features or transmission patterns for the different nodes or peer nodes. In this case, identifying node specific static and behavioral patterns over the aforesaid time-series data is must. On the other hand, in real-world application there can be the case where a node can keep transmitting continuously with normal traces, while certain sensor or node might transit quite rarely over certain event trigger. Such data condition can give rise to the class-imbalance and hence training any machine learning or deep learning models over such imbalanced traces can yield false positive or false negative performance. To alleviate such issues, training a model over active period and event-sensitive pattern is must. To achieve it, in this paper TCP Dump, a tool for capturing and analyzing network packets for traffic insights was applied to segment node specific features over corresponding time-series transmission traces. In order to segment the different traffic patterns over non-linear transmission scenario, $TCPDump$ tool was applied that extracted traffic traces to yield corresponding static features or allied dynamic network behavior. In this work, the use of TCP dump tool provided transmission records encompassing the information within the packet (from the MAC to the application layer of the WSN's IEEE 802.15.4 standard's open system interconnection). In reference to the real-time operating standards and the security protocols like Secure Sockets Layer (SSL), Transport Layer Security (TLS) and the privacy protection

policies by the different government agencies or lawmakers, only the packet header's information can be used for intrusion detection and classification. Nevertheless, the accessible information including the Source ID, the Destination ID, the Protocol used, medium access control (MAC) address, Packet size (i.e., the size of the transmitted data and the received data), delay information (i.e., the transmission period) etc. can be employed to classify the network traffic as the normal traffic or the malicious or intrusion traffic. It can further be used to detect the intruder node in the network. Noticeably, these details were obtained for each network traces (i.e., transmission records between the peer nodes) and thus the overall data comprised both normal as well as other six different kinds of intrusion cases, which were later used to train the model for multi-type intrusion prediction.

Unlike traditional intrusion detection systems, where the input patterns are directly mapped as input to the machine learning models for prediction, in the proposed model the input features (say, segmented network features) were processed for semantic feature extraction so as to retain more latent information about the network traces to perform multi-type intrusion prediction under uncertain transmission conditions. It seems to be more effective towards multi-type intrusion detection, where excessive transmission heterogeneity and non-linearity can't be ruled out. In this paper, we applied simple Word2Vec word embedding method that transformed input node features into the corresponding embedding matrix, which was later projected as input to the proposed cascaded deep network for learning and prediction. A brief of the Word2Vec model used is given as follows.

C. Word2Vec Semantic Feature Mapping

In this work, Word2Vec semantic feature extraction method also called as word-embedding was applied. More specifically, we applied Gensim Word2Vec method to transform input node features (sometime called tokens) into corresponding embedding matrix. In this work, the deployed Gensim Word2Vec model encompassed dual-layer neuro-computing mechanism embodying two hidden layers. This approach helped to yield more sparser features that consequently can help to reduce computational costs and hence can enhance overall resource efficiency and delay aspects of the Edge-IoT network. Thus, retrieving embedding output from each node and allied transmission traces or features, an embedding vector was obtained, which was mapped as input to the proposed cascaded deep network.

D. Cascaded Deep Network for Feature Extraction and Learning

In the past numerous efforts were made where the authors applied CNN or the RNN methods such as LSTM to perform feature extraction from the time-series data; however, almost major state-of-arts failed to address long-term dependency problem which can impact eventual learning and prediction output(s). A few approaches, especially applying CNN with the higher number of convolutional layers hypothesized to have achieved high-dimensional features; however, the likelihood of gradient vanishing over increasing convolutional layers can't be ruled out. Considering such inferences, for a robust multi-type intrusion detection system exploiting both local as well as contextual details was must, even ensuring alleviation towards gradient vanishing. In this reference, we designed a cascaded deep model encompassing LSTM and Bi-LSTM, where the first extracts the local features, while the later obtains the contextual features from the time-series data. Being cascade in design (Fig. 1), the output of the LSTM deep network is passed as input to the Bi-LSTM and eventually the output features from both (LSTM and Bi-LSTM) are mapped to the global average pooling (GAP) to yield composite hybrid deep feature. The obtained composite feature is projected to the fully connected layer that acts as a classification layer. In this work, Softmax classifier was applied with the cross-entropy cost function to perform multi-class classification and thus each network trace is classified for its types (i.e., normal, Fuzzers, DoS attacks, Wormhole attacks, Shell-code attacks, and Reconnaissance attacks). A brief of the deep network applied in this work is given as follows:

As depicted in Fig. 1, the proposed

cascaded deep network at first applies LSTM deep network. Noticeably, the key purpose of LSTM deep network development was to address the problem of vanishing effect and exploding gradient that improves efficacy of RNNs towards time-series data analysis and predictions [14]. The basic concept behind LSTM deep network is to control the cell-states by applying gates like input gate, forget gate and output gates. A typical functional design of an LSTM model is given in Fig. 2.

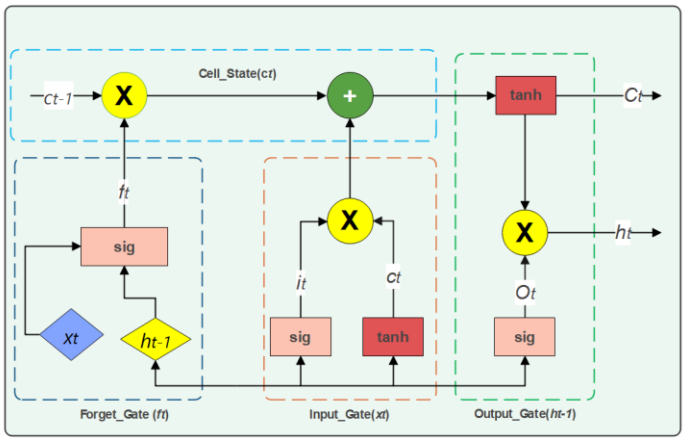

Fig. 2. A typical functional design of an LSTM model

The LSTM networks employ memory cells with gates for long-term dependencies to avoid vanishing gradient problems. A Bi-LSTM treats the sequence in both directions to enrich the context. LSTMs remember temporal information, making it quite suitable for data that is sequential. Bi-LSTMs incorporate past and future states into a contextual model and are therefore more sensitive, enhancing the model's robustness. Both architectures increase the accuracy of detection. Among these, Bi-LSTM yields finer contextual insight-which is necessary for the recognition of difficult temporal patterns.

In LSTM deep network, the forget gate (f_t) examines whether it requires storing the previous state's information (c_{t-1}) or forget it by applying the input (x_t) and the hidden state (h_{t-1}). The output of this gate can yield either 0 or 1. Similarly, the input gate (i_t) measures the level of information related to the input text (x_t) and the hidden layer (h_{t-1}) to be passed to update its cell-state for result generation (i.e., either as 0 or 1). The parameter c_t signifies the measured cell state by using mathematical functions on c_{t-1}, f_t and i_t. The information flow in between the current cell state to the hidden state is often controlled by means of the output gate (O_t) that usually exists as 0 or 1. Consider that at certain time t, the input data be x_t and its previous hidden state and cell state values be h_{t-1} and c_{t-1}, respectively. In the same manner, consider that the current output of the hidden state and the current cell state be h_t and c_t, correspondingly. Thus, the different gate elements

and their outputs are derived by using (1-5).

$$f_t = sigmoid\left(W_{fx}x_t + W_{fh}h_{t-1} + b_f\right) \quad (1)$$

$$i_t = sigmoid(W_{ix}x_t + W_{ih}h_{t-1} + b_i) \quad (2)$$

$$c_t = c_{t-1} \odot f_t + i_t \odot tanh(W_{cx}x_t + W_{ch}h_{t-1} + b_c) \quad (3)$$

$$O_t = sigmoid(W_{ox}x_t + W_{ch}h_{t-1} + b_0) \quad (4)$$

$$h_t = O_t tanh(c_t) \quad (5)$$

Fig. 2 forget gate (f_t) output

In above equations (1-5), $x_t \in R^n$ signifies the input vector, $W \in R^{v*n}$, $b \in R^v$, where n and v be the dimensions of the input vector and the number of words in the input data corpus, correspondingly. The selection of LSTM and Bi-LSTM networks for intrusion detection is well-founded due to their sophisticated architectural design, numerous benefits, and proven impact on enhancing detection accuracy. These models offer a powerful approach to understanding complex sequential data, making them ideal for identifying and mitigating network threats effectively. In this research work we are not considering transformers.

5.Results and Discussion

In this paper a novel and robust contextual deep semantic feature driven multi-type intrusion detection model (CDS-MNIDS) was proposed for Edge-IoT systems. The ability to extract event specific semantic features encompassing both local as well as contextual details make the proposed CDS-MNIDS model robust towards multi-type intrusion detection in Edge-IoT networks. In function, we considered UNSW NB15 dataset that comprises network traffic traces or transmission traces over a large number of autonomously operating IoT sensor

nodes. More specifically, in this work the transmission traces pertaining to the normal traffic, Fuzzers, DoS attacks, Wormhole attacks, Shell-code attacks, and Reconnaissance attacks were taken into consideration. The overall dataset was at first processed for network segmentation by using TCP Dump tool that obtained node specific features including node ID (source ID, destination ID), protocol used, data size, frame size, and delay. The proposed CDS-MNIDS intrusion detection model performed semantic embedding over the segmented node's features. More specifically, we applied Word2Vec embedding, a technique for representing words as numerical vectors and method by using Gensim method that transformed each node's features into equivalent embedded matrix. The extracted embedding matrix was passed as input to the proposed cascaded RNN encompassing LSTM and Bi-LSTM in sequence. The proposed model at first applied LSTM deep network to extract local feature from the embedding (feature) matrix, whose output was then passed to the Bi-LSTM to generate contextual details. Thus, extracted LSTM and Bi-LSTM features were mapped as input to the GAP layer that then generates a composite feature vector and feeds as input to the fully connected layer. The obtained features were processed for learning and prediction by using Softmax layer that in conjunction with cross-entropy cost function performs multi-class classification. To improve learning efficacy ADAM non-linear optimization function was applied, where the initial learning rate was assigned as 0.0001. Thus, the proposed model performed multi-class classification over the input feature vector and annotated each node trace as normal or attack classes (Fuzzers, DoS attacks, Wormhole attacks, Shell-code attacks, and Reconnaissance attacks). The proposed cascaded deep network annotated each node with respective type and respective confusion matrix was obtained.

The overall proposed model was developed by using MATLAB 2020b software tool. The proposed model was simulated over the central processing unit armored with the Microsoft Window operating systems, 8 GB memory and 3.2 GHz processor. The system configuration also embodied Intel i5 processor operating at 3.2 GHz frequency. The simulation results were obtained in terms of accuracy, precision, recall, F-Measure, time parameters. Noticeably, to achieve aforesaid statistical performance parameters, confusion matrix was obtained in terms of the true positive (TP), false positive (FP), true negative (TN) and false negative (FN). Here, the true positive (TP) values signified the instances moved correctly to the corresponding (correct) cluster. Moreover, false positive (FP) outputs indicate that the instance is moved to the wrong cluster, but labelled as correct. The mathematical formulations used to derive the different performance parameters are given in Table II.

Table II: Performance Parameters

Parameter	Mathematical Expression
Accuracy	$\frac{(TN+TP)}{(TN+FN+FP+TP)}$
Precision	$\frac{TP}{(TP+FP)}$
Recall	$\frac{TP}{(TP+FN)}$
F-Score	$2.\frac{Recall.Precision}{Recall+Precision}$

To assess robustness of the proposed CDS-MNIDS intrusion detection model, the performance characterization was done in terms of intra-model assessment and inter-model assessment. The detailed discussion of the simulated results and allied inferences is given in the subsequent sections.

A. Intra-Model Assessment

Since, in this work we hypothesized that the strategic use of LSTM and Bi-LSTM deep features be effective towards multi-type intrusion detection, we compared performance with LSTM features, Bi-LSTM features and fused LSTM and Bi-LSTM features. Here, the key motive was to assess relative efficacy of the different feature models. The simulated results are given in Table III.

Table III: Performance with the different feature model

Feature Model	Performance (%)			
	Accuracy	Precision	Recall	F-Measure
LSTM	96.68	97.84	97.03	97.43
Bi-LSTM	98.03	98.39	96.94	97.7
LSTM + Bi-LSTM	99.81	98.81	98.48	98.5

As depicted in Table III, we can observe that the use of LSTM deep network exhibits the intrusion detection accuracy of 96.68%. On the contrary, the use of Bi-LSTM feature resulted the intrusion prediction accuracy of 98.03%. Interestingly, the amalgamation of LSTM and Bi-LSTM deep features (say, cascade deep features) resulted the intrusion detection and prediction accuracy of 99.81%. The detailed assessment also indicates that the proposed hybrid (LSTM + Bi-LSTM) feature driven model achieves precision, recall and F-Measure of 98.81%, 98.48% and 98.5%. The overall results indicate that the proposed cascaded feature driven intrusion detection model exhibit superior, thus confirming superiority and suitability towards real-world multi-type intrusion detection solution for edge-IoT networks. The graphical depiction of the simulation results obtained are given in Fig. 3 to Fig. 6.

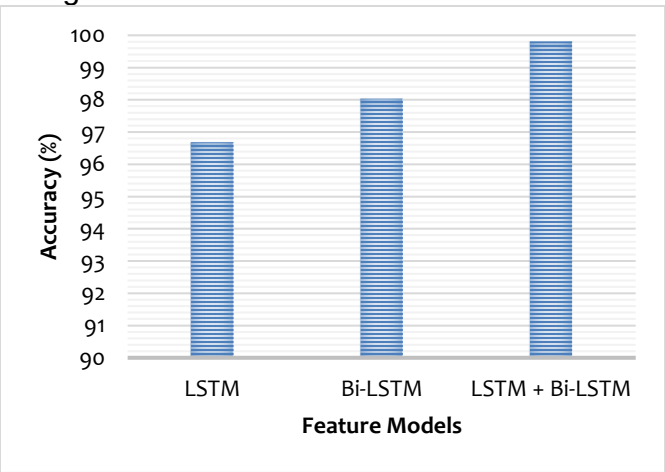

Fig. 3 Accuracy over the different feature models.

To assess whether the use of Word2Vec embedding model achieved superior efficacy over the normal pattern (i.e., without embedding) feature-based solution, we simulated the proposed model with and without embedding matrix. In other words, in addition to the proposed model where the Word2Vec embedded matrix was passed as input to the proposed cascaded deep network, we simulated by passing the original data directly to the proposed cascaded deep network. In this reference, the simulation results obtained are given in the Table IV.

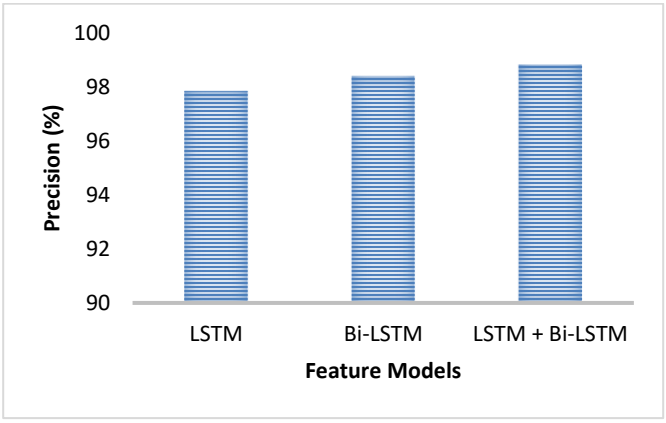

Fig. 4 Precision over the different feature models.

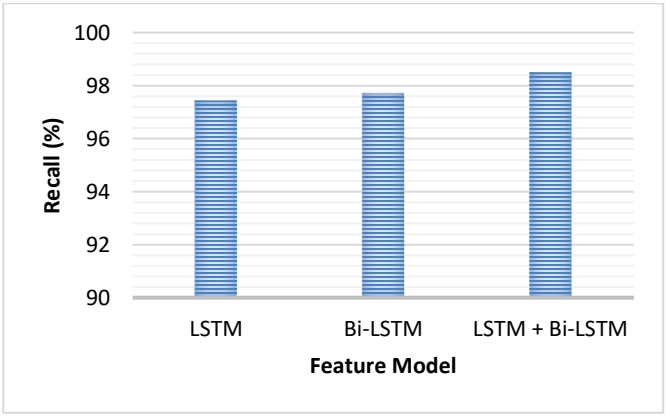

Fig. 5 Recall over the different feature models.

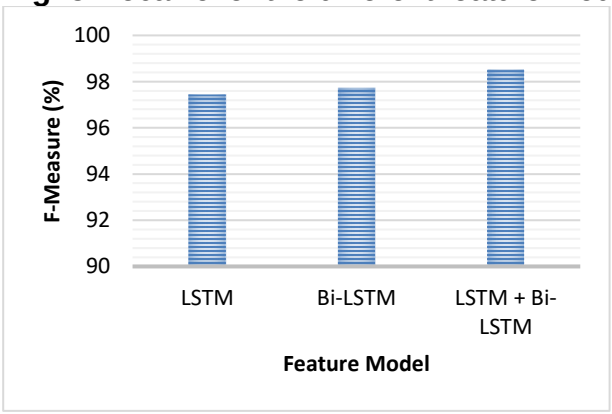

Fig. 6 F-Measure over the different feature models.

Table IV: Performance with the different input data nature

Feature Input	Performance (%)			
	Accuracy	Precision	Recall	F-Measure
Without Embedding	97.99	96.29	97.21	96.74
With Word2Vec LSTM + Bi-LSTM	99.81	98.81	98.48	98.5

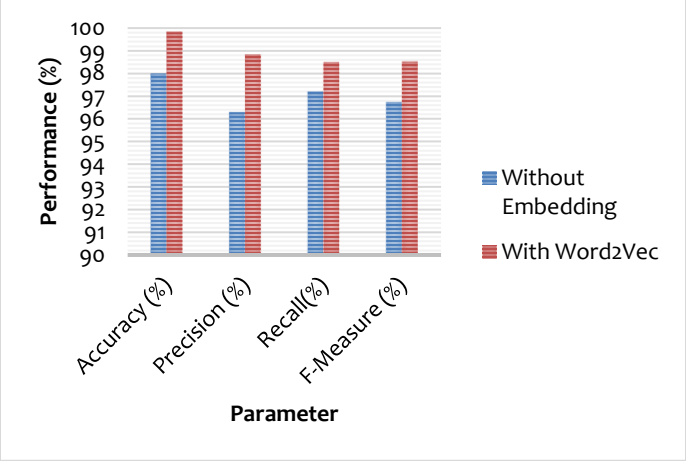

Fig. 7 Performance with and without Word2Vec embedding inputs

As depicted in above results, it can easily be found that the use of Word2Vec embedding driven method where key parameters include (size, window, min-count, and SG) cascaded deep network results intrusion prediction accuracy of 99.81%, while without embedding it results relatively lower prediction accuracy (i.e., 98%). Similarly, the F-Measure performance obtained too signifies the same result where it shows (F-Measure) value of 98.5% with Word2Vec embedding, while without embedding it shows F-Measure of 96.74%. The overall results confirm that the use of Word2Vec embedding as semantic feature extraction approach helps to achieve superior performance than without embedding driven feature learning.

B. Inter-Model assessment

To assess whether the proposed CDS-MNIDS intrusion detection model performs superior over the other state-of-arts we considered accuracy (%) as common parameter and the relative efficiency was measured for the different existing methods. In other words, we compared the performance with the different existing network intrusion systems. The relative performance outputs are given in Table V.

Table V :Relative Performance assessment

Reference	Accuracy (%)
[13]	96.00
[14]	92.90
[15]	97.14
[16]	89.02
[17]	99.67
[18]	98.30
[20]	94.00
[28]	85.20
[43]	99.62
[44]	83.58
[45]	99.80
[46]	97.85
CDS-MNIDS	99.81

Observing the overall results, it can easily be found that the proposed model performs superior over the other state of arts. Thus, in reference to the research questions, as defined in Section III, we can confirm that the strategic amalgamation of static as well as dynamic node behavior information be effective towards multi-type network intrusion detection in Edge-IoT systems. It confirms acceptance of the RQ1. Similarly, the research outcomes reveal that the use of Word2Vec semantic features obtained from the nodes' behavior pattern enable better feature extraction and learning to yield accurate and reliable intrusion detection system for Edge-IoT systems. It is confirmed in reference to the results obtained in the Fig. 8, and thus the RQ2 is found affirmative. The previous results (i.e., Table III) confirms that the use of cascaded recurrent neural networks be encompassing LSTM and Bi-LSTM deep networks in conjunction with global average pooling layer and fully connected layer yield reliable multi-type network intrusion detection and classification for scalable Edge-IoT network security, and therefore this research gives affirmative output or result for the RQ3. The overall research outcomes indicate the affirmative acceptance of the RQ1, which states that the amalgamation of static and dynamic network pattern driven semantic features, and cascaded LSTM Bi-LSTM network be effective towards multi-type network intrusion detection in Edge-IoT environment. LSTM and Bi-LSTM is a solid foundation for addressing gradient vanishing issues and

improving prediction accuracy. By exploring additional strategies such as regularization techniques, advanced architectures, hyperparameter tuning, data preprocessing, and ensemble methods, you can further enhance your model's performance.

6.Conclusion

With the high pace rising Edge-computing and allied IoT-enabled Edge communication (and application) services, guaranteeing reliability has become a challenge. Edge-IoT being complex and dynamic in nature can undergo network vulnerabilities due to the loosely coupled connections and man-in-the-middle attacks. Though, in the past, the different efforts are made towards network intrusion detection; however, almost all state-of-arts contributed standalone attack detection that doesn't fulfil the demand of a resource constrained Edge-IoT networks. Applying multiple intrusion detection tools for each attack types such as DoS, DDoS, Wormhole attacks, Fuzzers etc. can impose significant computational overheads and hence resource exhaustion, which can't be suggested for the (resource constrained) Edge-IoT systems. To alleviate such challenges, in this paper a novel and first of its kind contextual deep semantic feature driven multi-type intrusion detection model (CDS-MNIDS) was developed for Edge-IoT networks. The CDS-MNIDS security framework was designed in such manner that it extracts and trains over sufficiently large semantic features obtained from the temporal network logs to detect and predict multiple types attack conditions. In addition, it also targeted to address at hand challenge of gradient vanishing and long-term dependency, which is quite often ignored by major at hand network intrusion detection systems. In this reference, this research proposed cascaded recurrent deep network which could exploit both local as well as contextual (global) features from the network traffic data to perform multi-type intrusion detection. Technically, the proposed CDS-MNIDS model initially makes use of the Edge-IoT network traces obtained from the network gateway deployed over a large autonomously and coupled sensors. This work applied UNSW's IoT intrusion detection dataset, which was at first processed for network traffic segmentation, especially designed to alleviate any possibility of class-imbalance and over-fitting. The proposed CDS-MNIDS protocol obtained node's parameters such as node's address, packet size, source-destination information, transmission behaviour etc. as the node behaviour parameter to train the model for eventual outlier or multi-type intrusion detection and prediction. The segmented node features were then processed for Word2Vec embedding that resulted latent/semantic features to make learning even more efficient over unknown network conditions. Unlike traditional token-based feature, the use of semantic features strengthened the proposed model to achieve better learning and prediction. The semantic features obtained from the different node's parameters were fed as input to the cascaded RNN network encompassing LSTM and Bi-LSTM in sequence. Here, the LSTM model obtained local features from the input node features, while its output was passed as input to the Bi-LSTM for contextual feature extraction. Thus, the obtained local and contextual or global features were passed to the average pooling layer for further learning and prediction at the fully connected layer. This work applied cross-entropy cost function in conjunction with the Softmax layer to perform multi-type intrusion prediction. The simulation results confirmed multi-type intrusion detection accuracy of 98.96%, precision 98.21%, recall 96.87% and F-Measure of 0.975, which is higher than other intrusion detection models.

Reference

Abdullah, A., Alsolami, B., Alyahya, C. & Alotibi, C. 2018. INTRUSION DETECTION OF DOS ATTACKS IN WSNS USING CLASSIFICATION TECHNIUQES. *Journal of Fundamental and Applied Sciences,* 10**,** 298-303.

Abuadlla, Y., Kvascev, G., Gajin, S. & Jovanovic, Z. 2014. Flow-based anomaly intrusion detection system using two neural network stages. *Computer Science and Information Systems,* 11**,** 601-622.

Aburomman, A. A. & Ibne Reaz, M. B. 2016. A novel SVM-kNN-PSO ensemble method for intrusion detection system. *Applied Soft Computing,* 38**,** 360-372.

Ahmad, I., Basheri, M., Iqbal, M. J. & Rahim, A. 2018. Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. *IEEE Access,* 6**,** 33789-33795.

Al-Qatf, M., Lasheng, Y., Al-Habib, M. & Al-Sabahi, K. 2018. Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection. *IEEE Access,* 6**,** 52843-52856.

Beghdad, R. 2008. Critical study of neural networks in detecting intrusions. *Computers & Security,* 27**,** 168-175.

Butun, I., Österberg, P. & Song, H. 2020. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials,* 22**,** 616-644.

Casas, P., Mazel, J. & Owezarski, P. UNADA: Unsupervised Network Anomaly Detection Using Sub-space Outliers Ranking. *In:* DOMINGO-PASCUAL, J., MANZONI, P., PALAZZO, S., PONT, A. & SCOGLIO, C., eds. NETWORKING 2011, 2011 Berlin, Heidelberg. Springer Berlin Heidelberg, 40-51.

Chen, H., Meng, C., Shan, Z., Fu, Z. & Bhargava, B. K. 2019. A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation. *IEEE Access,* 7**,** 32853-32866.

Elbahadır, H. & Erdem, E. Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks. 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021. 401-406.

Elbasiony, R. M., Sallam, E. A., Eltobely, T. E. & Fahmy, M. M. 2013. A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Engineering Journal,* 4**,** 753-762.

Farivar, F., Haghighi, M. S., Jolfaei, A. & Alazab, M. 2020. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. *IEEE Transactions on Industrial Informatics,* 16**,** 2716-2725.

Farnaaz, N. & Jabbar, M. A. 2016. Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science,* 89**,** 213-217.

Gao, X., Shan, C., Hu, C., Niu, Z. & Liu, Z. 2019. An Adaptive Ensemble Machine Learning Model for Intrusion Detection. *IEEE Access,* 7**,** 82512-82521.

Gauthama Raman, M. R., Somu, N., Kirthivasan, K., Liscano, R. & Shankar Sriram, V. S. 2017. An efficient intrusion detection system based on hypergraph - Genetic algorithm for parameter optimization and feature selection in support vector machine. *Knowledge-Based Systems,* 134**,** 1-12.

Huang, H., Ding, S., Zhao, L., Huang, H., Chen, L., Gao, H. & Ahmed, S. H. 2020. Real-Time Fault Detection for IIoT Facilities Using GBRBM-Based DNN. *IEEE Internet of Things Journal,* 7**,** 5713-5722.

Jaber, A. N., Zolkipli, M. F., Shakir, H. A. & Jassim, M. R. 2018. Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing.

Jadidi, Z., Muthukkumarasamy, V. & Sithirasenan, E. Metaheuristic algorithms based Flow Anomaly Detector. 2013 19th Asia-Pacific Conference on Communications (APCC), 2013/8// 2013. IEEE, 717-722.

Jiang, F., Fu, Y., Gupta, B. B., Liang, Y., Rho, S., Lou, F., Meng, F. & Tian, Z. 2020a. Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security. *IEEE Transactions on Sustainable Computing,* 5**,** 204-212.

Jiang, S., Zhao, J. & Xu, X. 2020b. SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments. *IEEE Access,* 8**,** 169548-169558.

Kabir, E., Hu, J., Wang, H. & Zhuo, G. 2018. A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems,* 79**,** 303-318.

Khan, T., Singh, K., Hoang Son, L., Abdel-Basset, M., Viet Long, H., Singh, S. P. & Manjul, M. 2019. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. *IEEE Access,* 7**,** 58221-58240.

Kuang, F., Xu, W. & Zhang, S. 2014. A novel hybrid KPCA and SVM with GA model for intrusion detection. *Applied Soft Computing,* 18**,** 178-184.

Kumarshrivas, A. & Kumar Dewangan, A. 2014. An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set. *International Journal of Computer Applications,* 99**,** 8-13.

Lakhina, A., Crovella, M. & Diot, C. 2005. Mining anomalies using traffic feature distributions. *ACM SIGCOMM computer communication review,* 35**,** 217-228.

Latah, M. & Toker, L. 2020. An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks. *CCF Transactions on Networking,* 3**,** 261-271.

Lee, Y.-J., Yeh, Y.-R. & Wang, Y.-C. F. 2013. Anomaly Detection via Online Oversampling Principal Component Analysis. *IEEE Transactions on Knowledge and Data Engineering,* 25**,** 1460-1470.

Li, L., Yu, Y., Bai, S., Hou, Y. & Chen, X. 2018. An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k -NN. *IEEE Access,* 6**,** 12060-12073.

Li, T., Xie, S., Zeng, Z., Dong, M. & Liu, A. 2022. ATPS: An AI Based Trust-Aware and Privacy-Preserving System for Vehicle Managements in Sustainable VANETs. *IEEE Transactions on Intelligent Transportation Systems,* 23**,** 19837-19851.

Liao, H., Zhou, Z., Zhao, X., Zhang, L., Mumtaz, S., Jolfaei, A., Ahmed, S. H. & Bashir, A. K. 2020. Learning-Based Context-Aware Resource Allocation for Edge-Computing-Empowered Industrial IoT. *IEEE Internet of Things Journal,* 7**,** 4260-4277.

Liu, S., Guo, C., Al-Turjman, F., Muhammad, K. & De Albuquerque, V. H. C. 2020. Reliability of response region: A novel mechanism in visual tracking by edge computing for IIoT environments. *Mechanical Systems and Signal Processing,* 138**,** 106537-106537.

Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. & Lloret, J. 2017. Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT. *Sensors,* 17**,** 1967-1967.

Marir, N., Wang, H., Feng, G., Li, B. & Jia, M. 2018. Distributed Abnormal Behavior Detection Approach Based on Deep Belief Network and Ensemble SVM Using Spark. *IEEE Access,* 6**,** 59657-59671.

Mirsky, Y., Doitshman, T., Elovici, Y. & Shabtai, A. 2018. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection.

S. Liu, C. G., F. Al-Turjman, K. Muhammad, and V. H. C. De Albuquerque. 2020. Reliability of response region: A novel mechanism in visual tracking by edge computing for IIoT environments. *Mechanical Systems and Signal Processing,* vol. 138**,** p. 106537.

Song, S., Ling, L. & Manikopoulo, C. N. Flow-based Statistical Aggregation Schemes for Network Anomaly Detection. 2006 IEEE International Conference on Networking, Sensing and Control, 2006. 786-791.

Stevanovic, M. & Pedersen, J. M. An efficient flow-based botnet detection using supervised machine learning. 2014 International Conference on Computing, Networking and Communications (ICNC), 2014. 797-801.

Teng, S., Wu, N., Zhu, H., Teng, L. & Zhang, W. 2018. SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA Journal of Automatica Sinica,* 5**,** 108-118.

Tran, Q. A., Jiang, F. & Hu, J. A Real-Time NetFlow-based Intrusion Detection System with Improved BBNN and High-Frequency Field Programmable Gate Arrays. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012. 201-208.

Umamaheshwari, S., Kumar, S. A. & Sasikala, S. Towards Building Robust Intrusion Detection System in Wireless Sensor Networks using Machine Learning and Feature Selection. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021/10// 2021. IEEE, 1-6.

Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q.-V., Padannayil, S. K. & Simran, K. 2020. A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities. *IEEE Transactions on Industry Applications,* 56**,** 4436-4456.

Wahba, Y., Elsalamouny, E. & Eltaweel, G. 2015. Improving the Performance of Multi-class Intrusion Detection Systems using Feature Reduction. *CoRR,* abs/1507.06692.

Wang, H., Gu, J. & Wang, S. 2017. An effective intrusion detection framework based on SVM with feature augmentation. *Knowledge-Based Systems,* 136**,** 130-139.