A Zero-Trust Security Framework for Granular Insight on Blind Spot and Comprehensive Device Protection in the Enterprise of Internet of Things (E-IOT)

Anil G (gramaanil@gmail.com)
BMSIT: BMS Institute of Technology https://orcid.org/0000-0003-0610-8787

Research Article

Keywords: Internet of Things, Enterprise, Blind Spot, Zero Trust Security, Intrusion Recognition

Posted Date: June 14th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-476252/v1

Wirless Pers Commun

A Zero-Trust Security Framework for Granular Insight on Blind Spot and Comprehensive Device Protection in the Enterprise of Internet of Things (E-IOT)

Anil G N

Professor, Department of Computer Science and Engineering, BMS Institute of Technology & Management, Bangalore, India
Email: gramaanil@gmail.com

Abstract. The adoption of the Internet-of-Things (IoT) is swiftly rising in almost every aspect of human life, and its operational hardware is generating massive data. Also, cloud computing is an inherent operational technology of IoT for handling massive data because it has sufficient capabilities to store, process, and access control to the data. This brings several benefits, such as organizations increasingly depend on IoT to develop a smart approach to improve operational efficiency, automate complex tasks and provide quality-aware experience to their customer and end-user. As the number of interlinked devices increases, cybercriminals continue to look for blind spots and vulnerable devices in the network. Therefore, this paper attempts to introduce a zero-trust security framework to bring granular insight into the network and design effective intrusion identification methods to provide comprehensive and sustainable protection against dynamic attacks. The proposed framework comprises two implementation design aspects. Firstly, network modeling is carried out for complete visibility based on the number of connected devices and their behavior with other network devices. In this phase, the entire network is segmented into regions based on the IoT device's location to minimize the attack surface. Also, a lightweight cryptography-based secure data transmission mechanism is carried out for reliable communication. Secondly, an efficient machine learning-based intrusion identification system is developed to perform real-time monitoring and attack detection. The simulation outcome indicates the effectiveness of the proposed system for secure communication, data transmission, and attack detection. The comparative analysis demonstrated that the proposed zero-trust security system achieves an average of 35% resource efficiency anda 99 % accuracy rate in attack detection.

Keywords Internet of Things. Enterprise. Blind Spot. Zero Trust Security. Intrusion Recognition

1 Introduction

The tremendous growth in the regular usage of electronic and communication services has led to spectacular progress in the software technology, telecommunications sector, and hardware applications towards supporting the ubiquitous computation have emerged the concept of the Internet of Things (IoT). IoT refers to a multifaceted ecosystem composed of intelligent and context-aware devices that are facilitated with the skill to sense their environment, connect with each other, and exchange data over the Internet [1, -2]. With the advancement in cloud computing and sensing technology, IoT is fruitfully realized as a core component of Industrial 4.0 [3]. In recent years, we have witnessed the rise in IoT adoption in different enterprises such as smart homes, smart cities, healthcare, agriculture, transportation systems, and other enterprises [4]. IoT will boost enterprise efficiency by enabling diverse technological innovations by taking advantage of embedded devices with sensors and cloud platforms to support the demand of new business models and consistent physical operations with digital resources in real-time [5-6].

According to the Ericsson mobility report, by 2022, there will be more than '30' thousand million connected devices in regular use. Approximately'18'thousand million devices will be used in various IoT applications[7] like digital healthcare for patient monitoring, vending equipment, and many more devices particular to a specific context. In a report published by Forrester, 77% of companies confess that IoT devices' increasing usage poses significant security challenges [8]. Therefore, it is expected that as the number of connected devices continues to increase, the challenge for an enterprise system to protect them from potential threats and dynamic attacks will be a very challenging task. The IoT ecosystem is associated with heterogeneity, resource constraints, the varied nature of access devices, and different communication technologies and protocols. These connected devices are suffering from various vulnerabilities, which makes potential attack surface to attract cyber-attacks [9] and also invites malware, airborne threats like the case of WannaCry ransom ware attacks [10] and BlueBorne [11]. In the years may 2017, 2 lakh 30 thousand computers were infected with ransom ware attacks across 150

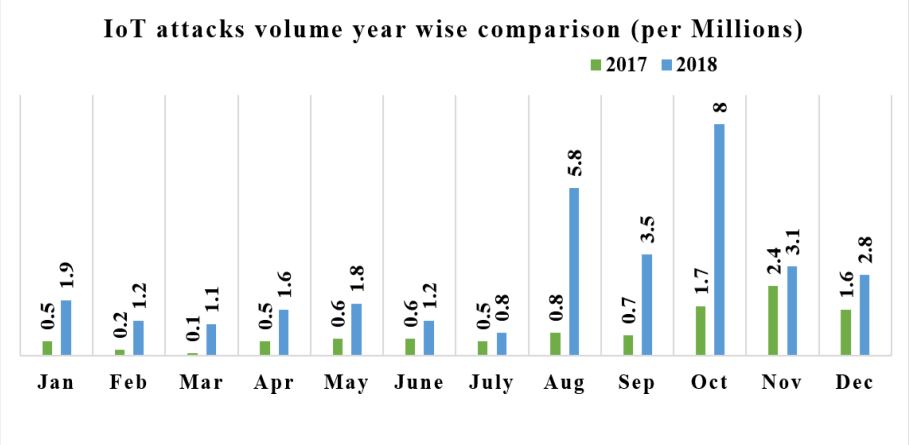

Fig. 1 IoT attacks volume year-wise comparison

Countries in one day. BlueBorne are an attack that enables cybercriminals to take advantage of vulnerabilities in Bluetooth. As shown in Fig 1, the cyber-attacks on IoT devices increased during 2018 from 10 million in 2017 to 32 million, according to the security threat report 2019 [12].

Although IoT brings exciting benefits to many enterprises, the security of IoT devices must not be ignored. Otherwise, it may develop into a blind spot, leading to adverse impacts on the entire network. Moreover, the significant facts about IoT device vulnerability are that that adversary can gain unauthorized access without knowing the concerned entity. If it is unknown that what all the devices are connected to the network and the risk factor associated with IoT devices, it will be very difficult to know when the network defense system is compromised and how to recover it from the impact of attacks. Therefore, it is required to ensure complete visibility of IoT devices connected to the network. An effective mechanism is required to develop that can perform real-time monitoring and detection of potential threats. Over the years, many research studies and surveys have been conducted in this field to address potential threats and security attacks [13-14]. However, still to date, a comprehensive security solution in IoT applications is missing in the existing literature. The solution based on cryptography primitives provides good security features but at the cost of computational complexity, which is not suitable for the resource constraint devices in the IoT ecosystem. Another interesting factor is that the existing solution has not considered responsible parameters associated with their security designs. To achieve particular requirements and meet specific objectives, the existing schemes lack other crucial requirements concerning quality-of-service aware communication and data transmission. Also, the design of existing multipath routing schemes is not adequality designed considering IoT networks' characteristics [15].Still, the existing routing approach for IoT is designed based on the principle of conventional routing schemes and mostly by considering the wireless sensor network's characteristics, which is entirely different from the IoT. The existing literature also lacks efforts to reduce the network's attack surface and lacks an effective mechanism of complete visibility of their network status and node behaviors. This factor introduces a blind spot in the network, which becomes a major vulnerability and invites potential threats. However, many Intrusion Detection Systems (IDSs) based on machine learning technologies have been introduced in the existing literature [16-17]. These IDS are very effective for detecting attacks for which they are trained from the specific dataset. However, most of the existing IDS are trained on the conventional dataset and lacks considering recent or dataset related to IoT context.

Therefore, this paper intended to introduce a zero-trust security model, which means no trust and only assesses the security status and risk associated with every physical and virtual network component followed by the second line of the defense system. To achieve zero-trust security in IoT networks, this paper introduces a dynamic and multi-layer security model. The proposed security model's overall design is carried out in multiple phases, i) Network segmentation phase and secure communication, and ii) Lightweight and centralized intrusion recognition system based on the deep learning approach. In the first phase of implementation, the attack surface is reduced, workload among nodes is controlled and distributed by segmenting the network into multiple regions. In this phase, reliable communication is also ensured by introducing a key-sharing-based multi-hop routing scheme. In the second phase of security implementa-

tion, an effective intrusion detection system is designed to provide real-time monitoring of network security status. This part of implementation also enables a mechanism to support the construction of the risk profile. The risk profile is maintained based on the result provided by proposed intrusion detection and the collection of data related to IoT devices and details about the third-party application running on the IoT devices. Based on the risk profile, a concerned entity or security administrator able to analyze the risks and vulnerabilities in the network and effectively takes a pro-active action before such risk and vulnerability come into any malicious action.
The rest of the sections of this paper are organized as follows: Section-2 presents related work. Section 3 proposed system design followed by algorithm description. Section 4highlights outcomes achieved and discuss the performance of the proposed system based on the comparative assessment. Finally, the contribution and overall scope of the proposed work are concluded in Section 5.

2 Related Work

Various research studies have been conducted in recent years to ensure effective security implementation in IoT-based network applications. Various systematic investigational studies and reviews are conducted by authors [18-19] for trust assessment and fault analysis in the IoT ecosystem. The authors in [20] discussed the mechanisms for the detection of attacks in the fog-things architecture. This paper highlighted the usage of a neural network to detect four different attacks and anomalies. The work carried out by [21] highlighted the challenges associated with security and privacy during data transmission between the physical IoT devices and virtual components of the cloud. The authors have suggested a digital watermarks-based data privacy mechanism. In the study of [22], the authors have explored the effectiveness of an intrusion detection system, where several machine learning classifiers have been considered for network scanning, probing, and Denial of Services attacks. A synthetic dataset is used to perform modeling of intrusion detection. The researchers in [23] introduced a system of classification-based recognition service enabled with cloud computing. In this paper, an extreme learning machine is employed with Net flow formatted data for scanning and control a compromised host. The use of a combined approach of recurrent and convolution neural networks are found in the study of [24] to handle the problem of over fitting, and modeling is carried out with a subset of features. The researchers in [25] suggested multi-directional Recurrent Neural Network and performed feature engineering to normalize and transform categorical features to numeric feature values. The authors in [26] adopted a deep neural network-based intrusion detection model considering the NSL-KDD dataset. Stochastic gradient descent is considered for the loss function. This study considers fog nodes to train the learning model. Artificial Neural Network isused in [27] to detect Distributed DoS attacks using the Bot-IoT dataset. SMOTE technique is adopted to normalize the dataset, and feature normalization is carried out before providing training to the learning model. The extensive review work presented in [28] discussed different security attacks in IoT and highlighted various intelligent solutions and challenges. This study also identified a research gap to provide a significant research direction.

3 Proposed System

This section presents the modelling of the proposed zero-trust security framework. The core objective of this study is to address the issues of blind spots (such as uncertainty, hidden vulnerabilities, and anonymous compromised nodes in the network). The goal is to achieve a zero-trust security mechanism towards ensuring seamless communication and reliable data transmission in the critical applications of the enterprise. The entire contribution is proposed in two phases of implementation. The first phase discusses the network modelling to reduce the network attack surface in the network by segmenting it into multiple regions and energy-efficient secure multipath routing strategy using lightweight cryptography operation. The second phase of this proposed system an intelligent and efficient intrusion recognition system to carry out real-time monitoring and alert system when any attacks are found. The study also discussed the conceptual modeling of risk profiling.

3.1 Network Modelling

The study implements an ideology of the network segmentation process in order to diminish attack surfaces to a significant extent and enable precise control of network traffic and distribution of workloads on IoT devices. The prime consideration behind this approach is that there is maximum possibility of attacks in an un segmented network, and also, a single event of attacks cans a severe impact on the entire network performance. Therefore, the more the network is divided, the more difficult it is for hackers to use the IoT device as a single point of network attacks and performance degradation. Another significant advantage of network segmentation is the distribution of workload on IoT devices, leading to achieving energy efficiency in the network. Apart from network segmentation, a secure multi-hop routing is introduced to efficiently and securely carry out the data transmission process. Security is ensured by sharing the lightweight secret key to IoT devices via a gateway. The modeling of network segmentation and secure data transmission is discussed as follows:

3.1.1 Network Segmentation and Secure Communication

In the initial setup of network modeling, n number of IoT-devices nodes is placed randomly in the deployment region. The study considers a case study of E-IoT; the network is dispersed with heterogeneous IoT devices with their unique identifier provided via IoT gateway. The study considers IoT-gateway as a centralized controller for the IoT devices, which maintains the records of information about the network status, IoT devices, and their behavior with the adjacent devices and provides fast and complete device discovery. This process also acts as the initial layer of proposed zero-trust security for ensuring the non-existing of any blind spot in the network. In this regard, the gateway provides a unique identifier and request to IoT devices to broadcast their position information. Each IoT-device gets a message from the gateway node and store in their routing table. Also, each device maintains a routing table based on the updates of their adjacent device conditions. Afterward, the segmentation of the network is carried out on the basis of distance factor (Df) using cutoff value numerically expressed as follows:

$$\mathrm{Df} \rightarrow (\mathrm{r}-1)\delta < \mathrm{R_r} < \delta r \ldots \text{(eq.1)}$$

Where r indicates segmented network region $(r = 1,2,3 \dots n)$ and δ cutoff distance factor. Similarly, network segmentation is carried out with n number of r (segmented region) and connected and controlled via a centralized component gateway. The IoT devices in the segment network region closer to the gateway require less transmission power and energy to forward sensed data. The segmented network region that is not much closer to the gateway uses their intermediate or closer segmented regions to forward their data in a power-efficient manner. Also, the proposed system considers the grouping of IoT devices based on the approach of the k-nearest neighbor (KNN) technique, where a grouping of IoT devices is carried based on the K nearest adjacent devices using the lightweight distance formula. K is determined by computing the square-root of the IoT device in the particular segmented network region (r). Figure 2 depicts the segmentation of the network in various regions. The group of devices also assigned with a unique identifier to address them from the other groups in the same segmented network region. In order to utilize network resources optimally, the system introduces a mechanism of choosing group leader as a data-packet forwarder, which is a virtual device allocated at a centroidal point in each network groups, numerically expressed as follows:

$$g(p,q) = \frac{\sum_{i=1}^{j} p_i}{N} + \frac{\sum_{i=1}^{j} q_i}{N} \dots \text{(eq.2)}$$

Where g is the particular group of the set of IoT devices $\{n_1, n_2, n_3, \dots n_j\}$, and p, q is the IoT devices localization coordinates, and N is the total IoT devices with groups.

Algorithm 1: Network Segmentation and Communication

Input: IoT devices (n)
Output: Efficient Routing
Start

1. Initialize n
2. Perform deployment
3. Compute distance along with adjacent n
4. Node maintains routing table: T
5. Distance factor Df $\rightarrow (r-1)\delta < R_r < \delta r$
6. **for** each device ϵ [1: Df] **do**
7. Segmentation network into particular regions: r
8. **end for**
9. check: $r_i[\,]! = \text{Null}$**do**
10. group formation in each segmented region using k-NN
11. **end check**
12. **for** each $n_i \epsilon\, r_i$
13. Compute: $g(p,q)$
14. Select data packet forwarder device
15. **end for**
16. **end procedure** for network segmentation

End

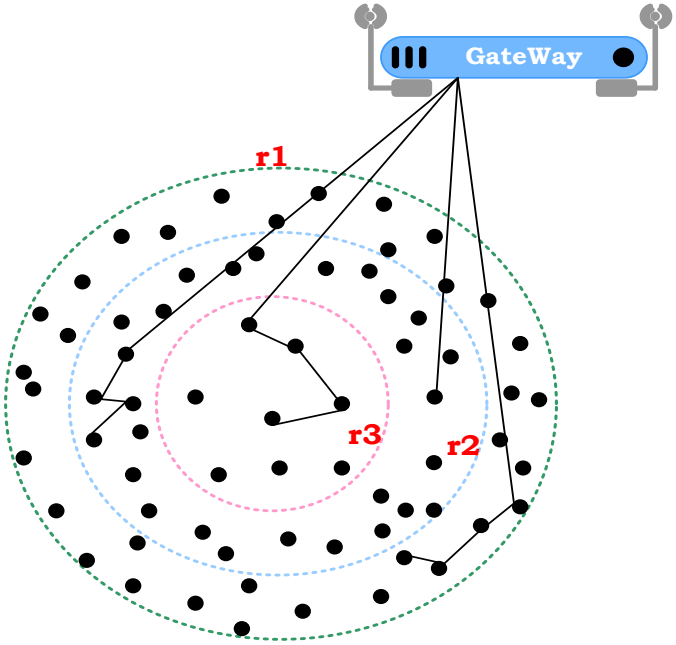

Fig 2 Network segmentation in different regions

3.1.2 Security Modelling

This phase of modeling ensures efficient security during the data communication process. In this implementation, lightweight and computationally efficient secret key is shared with each IoT device based on the XoR operation. Initially, the 'n' number of random secret keys is generated by the IoT gateway and transmitted to each IoT device in the corresponding network segmented region. The size of each key is equal to the size of k-bits data. The packet P from region rn with k size via the forwarder device is encrypted with network segmented region key by computing XoR operation numerically expressed as follows:

$$E = s_{s_{key} \oplus P} \ldots \text{(eq.3)}$$

In the next step, the encrypted k-bit size packet of a particular network region (rn) is forwarded to the intended data forwarder IoT device of the next-associated network region (rn-1). Then again, the packet P is encrypted using the current network region rn-1secret key. In a similar way, this process continues till it reaches its destination or IoT gateway node. Upon receiving data packets, the IoT- gateway decrypts (D) the packets by executing XoR operation considering all secret-key s_{key-i}, numerically expressed as follows:

$$D = S_{key-1} \oplus S_{key-2} \oplus S_{key-3} \ldots \oplus E_n \ldots \text{(eq.4)}$$

Algorithm 2: light-weight cryptography XoR operation

Input: IoT devices (n)
Output: Secure data transmission
Start

1. **Procedure data security**
2. Gateway provides n random S_{key-i}
3. S_{key-i}→ data forwarder device in the corresponding region: r_i
4. Encrypt data-packet with r_i key
    a. $E = s_{s_{key} \oplus P}$
5. The process will continue with intermediate:r_i
6. Upon receiving an encrypted data packet at the gateway
7. Decryption D
    a. XoR with a set of S_{key-i}
8. **End**

3.2 Real-Time Network Monitoring

The proposed system introduces an Intrusion Recognition System (IRS) for real-time monitoring of network security status. The proposed IRS design is lightweight that can comply with the processing capabilities of the constrained devices. In this paper, the study adopts the centralized architecture of lightweight IRS by considering that it is not feasible to implement an active agent for intrusion recognition in each IoT device due to limited resources. Therefore, a centralized IRS is developed and implemented on the network layer above the IoT-gateway component to alleviate resource constraints and heterogeneity issues. Figure 3 depicts the typical functioning of the proposed Light-weight and Centralized Intrusion Recognition System (LC-IRS). The proposed LC-IRS consists of core operational modules, namely, traffic/event collector, behavior analyzer, and alarm, to perform real-time monitoring and reporting and alert the concerned entity to manage the risks identified in the ecosystem E-IoT.

3.2.1 Traffic/Event Collector

This module of the proposed LC-IRS gathers and accumulates all the real-time events concerning network traffics, IoT device behavior with their adjacent devices, and weighing the cost of each device. This module also builds a behavior profile that can be represented in the form of a vector, numerically expressed as follows:

$$\overrightarrow{B_i} = \{e_1, e_2, e_3 \cdots, e_n\} \ldots \text{(eq.5)}$$

where,$\overrightarrow{B_i}$Indicates behavior profile in the form of the feature vector, which is a collection of real-time events (e) concerning trafficdata of IoT devices.

3.2.2 Behavior Analyzer

This is the core module of the LC-IRS, which analyzes and detects intrusions. The design and development of the Behavior Analyzer module are based on the analytics engine enabled with Deep learning functions to perform the classification of normal traffic and abnormal traffic (Attack). It also maintains a local repository for storing data

associated with the current behavior of devices for computing risk profiles. A detailed description of the risk profile is given in the next section.

3.2.3 Alarm

After attack recognition, LC-IRS blocks the compromised devices, terminates their participation in the network operation, and sends an alert notification to the concerned security administrator for further action.

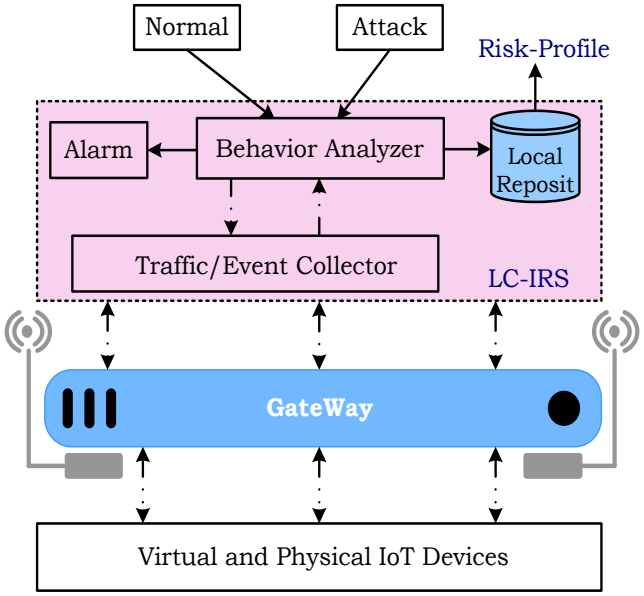

Fig 3 The typical functioning of the LC-IRS for real-time monitoring of network status

3.3 LC-IRS Implementation

This section discusses the design of the analytics engine functioning in the Behavior Analyzer module of the proposed LC-IRS. The core design of the analytics engine is based on the explicit approach of the deep learning technique to classify normal traffic and attack events. The proposed mechanism consists of multiple phases such as dataset preprocessing, feature engineering and selection, dataset split in training and testing set, and event classification using Convolution Neural Network (CNN). Figure 4 depicts the schematic architecture of the Behavior Analyzer of the proposed LC-IRS for intrusion recognition.

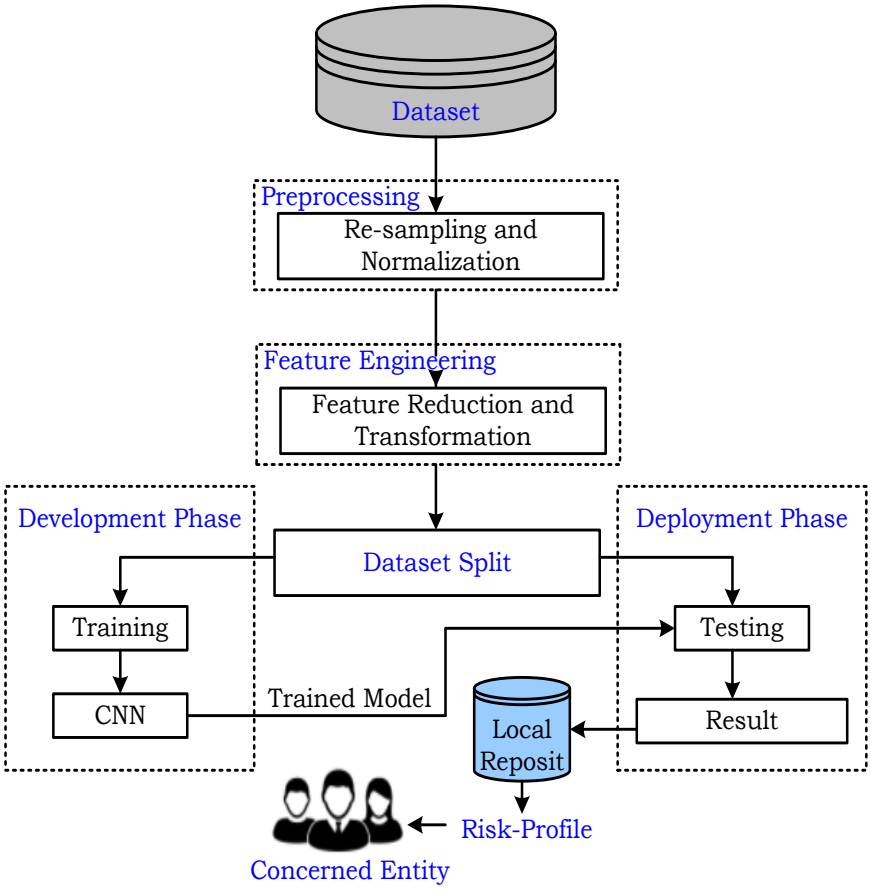

Fig 4 Analytical Behavior Analyzer of the Proposed LC-IRS

3.4 Dataset

The study considers the Bot-IoT dataset developed by Koroniotis et al.[29] in the year 2018 in the cyber center of UNSW. A virtual testbed is a setup by the authors to captures normal and malicious traffic data from the simulated experiments of IoT devices for smart home applications. The Bot-IoT dataset consists of more than 73 million events labeled as normal and attacked. Table 1 lists a few samples of the feature of events captured in the Bot-IoT dataset. However, there are42 attributes in the Bot-IoT dataset. The attacked events are categorized into 4 different classes as Denial-of-Service (DoS), Distributed DoS, information theft, and reconnaissance attack. The statistical observation of each class of attacks is separated into subgroups, as mentioned in Table 2.

Table 1 Sample representation of features of captured traffic events in the Bot-IoT

Features	Datatype	Description
pkSeqID	Packet sequence identity	Row identifier
stime	Float	Event start time
proto	Transaction protocols in Textual form	Category
Saddr	Source IP address	Category
Sport	Source port number	Category
Daddr	Destination IP address	Category
Dport	Destination port number	Category
Pkts	Total count of packets in transaction	Integer
Bytes	Total number of bytes in transaction	Integer
State	Transaction state	Category
Ltime	Event Last time	Float
Seq	Argus sequence number	Integer
Dur	Record total duration	Float
Mean	Mean duration of aggregated events	Float
Stddev	Standard deviation of aggregated events	Float
Sum	Total duration of aggregated records	Float
Min	Minimum duration of aggregated records	Float
Max	Maximum duration of aggregated records	Float
Spkts	Source-to-destination packet count	Integer
Dpkts	Destination-to-source packet count	Integer
Sbytes	Source-to-destination byte count	Integer
Dbytes	Destination-to-source byte count	Integer
Rate	Total packets per second in transaction	Float
Srate	Source-to-destination packets per second	Float
Drate	Destination-to-source packets per second	Float
TnBPSrcIP	Total number of bytes per source IP	Integer
TnBPDstIP	Total number of bytes per destination IP	Integer
TnP_PSrcIP	Total packets per source IP.	Integer
TnP_PDstIP	Total packets per destination IP.	Integer
TnP_PerProto	Total number of packets per protocol.	Integer
TnP_Per_Dport	Total number of packets per Dport	Integer

Table 2 Statistical attributes of Bot-IoT

Events Captured	Class	Sub-class	No. of events
Normal			9543
Attacks	DoS (52.25%)	TCP	19,547,603
		UDP	18,965,106
		HTTP	19,771
	DDoS (44.98%)	TCP	12,315,997
		UDP	20,659,491
		HTTP	29,706
	Information theft (0.22%)	Keylogging	1,469
		Data exfiltration	118
	Reconnaissance (2.48%)	Service scanning	1,463,364
		OS fingerprinting	358,275
Total Events Captured			= 73,370,443

3.5 Dataset Preprocessing

Since the proposed scheme is designed considering real-world IoT scenarios, network traffic events are captured and maintained in different formats, dimensionality, and highly associated with noise. Therefore, data preprocessing in this regard is the crucial step towards obtaining adequate and linear performance in the behavior in the classification problem. In this paper, data preprocessing operation deals with data resampling and normalization. From table 2, it can be analyzed that there only 9,543 events are only associated with normal class, and 73,360,900 events are the attacks classes. It can also be noticed that most of the events, i.e., approximately 96%, are subjected to DoS and DDoS attack classes. This factor can lead to a proposed model biased towards learning majority attack classes and misleading in identifying the normal and minority attack classes. The proposed study adopts the resampling approach of the synthetic minority oversampling mechanism. It is quite suitable to deal with multi-context events in a dataset of categorical and continuous features. As a result, fewer sampled events associated with normal class and theft-information attacks are augmented to 1000000 samples. Afterward, the dataset is normalized with a mix-max scaling approach in the range of [0,1], numerically expressed as follows:

$$Z = \frac{X - \min(X)}{\max(X) - \min(X)} \ldots. \text{(eq.6)}$$

The process of data normalization leads towards optimization in the model learning by ensuring less variance in convergence problems and makes the learning process less subtle at the functional scale.

3.6 Feature Engineering

This section discusses the process of feature space reduction and transformation. This process is carried out to maintain the computational efficiency of the proposed LC-IRS. The size of features of the dataset samples is quite large, which requires approximately

3 GB of storage cost, which may also lead to proposed LC-IRS suffers from computation complexity while executing the learning and testing process. In this regard, feature space reduction helps to reduce the computational resource requirement and boots the training and intrusion recognition process. In this context, the first process is carried out towards transforming features sample of object data-type into 13categorical data-types. The object data-type are regarded as features that require large storage costs. In the next step of feature space reduction, the 64-bit long integer data type is mapped to the 32-bit integer without any truncation errors. This process results in a significant reduction of huge storage or memory cost requirements. The proposed study also considers avoiding un-significant feature samples like i) 'pkSeqID′packet sequence identity similar to the index generated automatically, ii) ′stime′event start time and iii) ′ltime′event last time, both are available in the ′stime′ overall duration feature.The entire process significantly reduces 70% of the memory cost requirements. Afterward, data split process is carried out where 80% dataset is considered for a training data sample and 20% dataset is considered for the testing data sample. Further, transformation is applied to the training data samples. In training, data samples 30 numerical features that contain discrete as well continuous feature values. However, the discrete feature values do not need any transformation process. But there are 28 continuous values in the training dataset that require the transformation operation process because continuous values are highly associated with non-uniformity, which may severely degrade the performance concerning linearity in the detection and classification process. Therefore, this problem on non-uniformity is handled by using log-transformation followed by a standard normal distribution. The log transformation to get a new training data sample can be numerically expressed as follows:

$$K' = \log 10k \ldots \text{(eq.7)}$$

Where k indicates input training data samples and k' is the new value of the training data samples obtained after log base 10 transformations. Further, k' is processed with the standard normal distribution that scales the training data samples to the unit variance, numerically expressed as follows:

$$k'' = k' - \frac{\mu}{\sigma} \ldots \text{(eq.8)}$$

Where, k'' is the final version of normalized training data samples fed to the classification module to perform traffic event classification and attack detection, μ is mean, and σ is the standard variation.

3.7 Model Training and Classification

The proposed model training and traffic event classification is carried out using the deep learning approach of CNN. The CNN is a specific class of deep neural networks composed of multiple layers, where the input layer first layer of CN model, the hidden layer, and layer is the output layer. The hidden layer exists between the input, and the output layer that executes convolution and pooling operations. In CNN, the hidden layer, also called as the convolution layer, which has a set of kernels and is regarded as sliding filters over the input data that produces a feature map. Similarly, the pooling

layer is executed on the feature map for the purpose of dimensionality reduction by using a subsampling process over the featuremap. Figure 5 presents the architecture of the CNN model adopted in the proposed study.

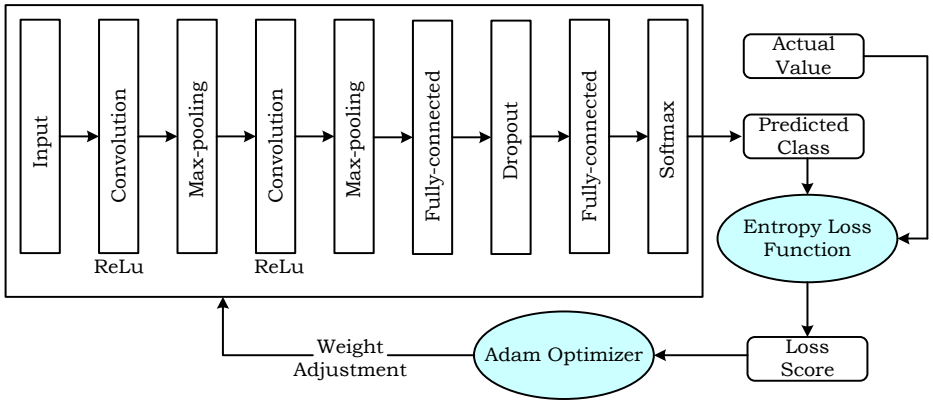

Fig 5. Proposed CNN model for attack detection

Figure 5 depicts the schematic of the proposed CNN model for feature learning and behavior classification. The proposed CNN model is configured with one input layer, two convolution layers, two dense layers, and an output layer with a softmax function for multiclass prediction. ReLu is used as an activation function at each convolution layer, and max pooling and dropout are used to overcome the issues associated with over fitting. The study considers the cross-entropy loss function and Adam optimizer to update weighting paraments of the learning model of LC-IRS. The configuration details are highlighted in table 3.

Table 3 Configuration details of CNN Hyper parameters

SI. No	Hyper parameters	Values
1	Convolution layer-1	Filter = 64,and size = 3x3
2	Convolution layer-2	Filter = 128,and size = 3x3
3	Max-pooling layer	2, filter size 2x2
4	Activation function	ReLU
5	Dropout offset	Flattening
6	Dropout probability	0.3-0.5
7	Output layer	Softmax
8	Training and Testing ratio	80% and 20% respectively

Algorithm 3: LC-IRS for normal behavior and attack recognition

Input: Traffic data (T_D)
Output: Traffic event class prediction: Normal/Attack
Start
1. Load: Input data
2. **for**I =1: T_D **do**

3. Preprocessing
    a. Resampling
    b. Normalization
4. **end** for
5. **While** T_D→normalized **do**
6. Process feature engineering
7. Execute: feature space reduction
    a. Convert object data type → categorial
    b. Map 64-bit long integer →32-bit integer
8. **While** done
9. Split T_D→ [k, P]
    // k- Training sample dataset
    // P- Testing sample dataset
10. for all continuous values ϵ k **do**
11. Transformation
    a. $k' = \log 10k$
    b. $k'' = k' - \frac{\mu}{\sigma}$
12. **end** for
13. Process **model development**
    a. Input = Layer (shape=[1])
    b. C1 = layer (size=64, connect = input)
    c. C2 = layer (size =128, connect = C1)
    d. Output = layer (shape = 2, connect = C2)
14. Train the model
    a. Optimizer = Adam ( )
15. Model = model.train(CNN, k″)
16. **While** training done **do**
17. Process **model deployment**
18. Select: T_D← P
19. if: model prediction **done**
20. **Check:** Predicted Outcome
    a. if: accuracy is higher
    b. Otherwise: adjust hyper parameters
    c. Train and test again
21. Evaluate performance

End

The proposed system LC-IRS also maintains a local repository for storing data associated with the current behavior of devices for computing risk profiles. A detailed description of the risk profile is given in the next section.

3.8 Risk Profiling

This section discusses the conceptual design of the risk profile for pro-active defensive actions against security risk and threats regarding the proposed security model. The risk profile is a supplementary component of the proposed zero-trust security framework, which will offer concerned security authority building a proactive strategy to mitigate

the impact of unforeseen and unethical actions in the network in advance based on future risk estimation. Typically, the risk is defined as the possibility of vulnerability and its adverse impact. It can be numerically expressed as follows:

$$R = L_V + I \ldots \text{(eq.9)}$$

Where the variable L_V likelihood of vulnerabilities, and variable I is the impact, i.e., the marked influence of the estimated network vulnerabilities. In the proposed work, the risk profiling is carried out based on the sub-profiling, such asi) Intruder profile ii), Device profile, iii)Web profile.

3.8.1 Intruder Profile (LC-IRS Predicted Outcomes)

The entire predicted outcome obtained from the proposed LC-IRS is stored and maintained in the local repository of the proposed zero-trust security framework. This information helps to determine the future risk based on the estimation of the number of cyber-attacks being introduced to the network or identified by LC-IRS, the kind of attacks, and the frequency of the attacks. Basically, all the information is stored with their timestamp and represented in a vector that can be regarded as an intruder profile I_p, numerically expressed as follows:

$$I_P = \{N_{Attack}, A_{type}, F_{Attack}\} \ldots \text{(eq.10)}$$

Where, I_P is the intruder profile, which is a collection of the number of attacks being detected (N_{Attack}), class or type of attack (A_{type}), and frequency of attacks that have occurred in the network (F_{Attack}).

3.8.2 IoT-devices profile (Device Categories and Associated Traffic Log)

The enterprise IoT ecosystem is a collection of various heterogeneous devices specific to different application sectors. Therefore, the entire information related to IoT devices and their associated traffic logis maintained in the local repository. This profile represents the risk vectors of the IoT devices in each network sub-region which depends on the various critical parameters, numerically expressed as follows:

$$D_P = \{D_{type}, D_{ED}, D_{P\&D}, D_{SL}, D_{TL}\} \ldots \text{(eq.11)}$$

Where, D_P is the IoTdevice's profile, which is a collection of multiple vectors that include types of IoT devices (D_{type}), IoT device's external dependencies (D_{ED}), IoT device's patches and upgrades ($D_{P\&D}$) by the manufacturers, IoT device's security level (D_{SL}) that related to the degree of authentication and credentials, IoT device's traffic log (D_{TL})that includes the timestamp of access, geographical location, IP addresses, and data requested.

3.8.3 Web profile (Vulnerabilities Associated with Third-Party Application)

In E-IoT, many third-party applications run on IoT devices. In this regard, the proposed system also maintains web-profiling, holding information on vulnerabilities related to the third-party applications and exceptional risks associated with IoT device's firmware. The web profiling (W_P)will be carried out based on the information collected using queries requested to multiple public sources such as the Mitre framework that offers common knowledge about adversary tactics. Figure 6 depicts the schematic architecture of the conceptual risk profiler.

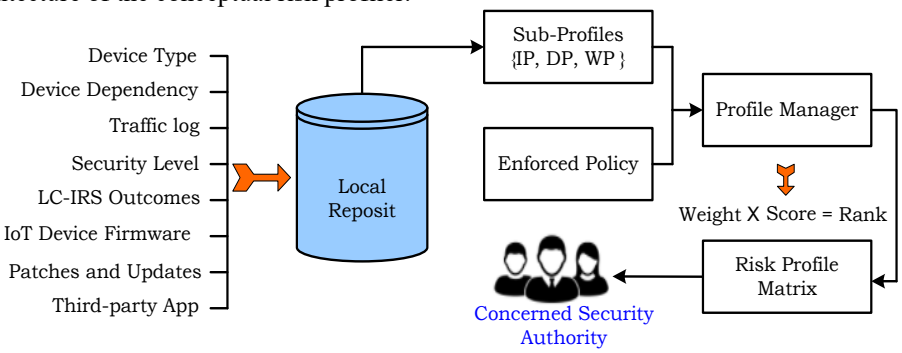

Fig.6 Schematic architecture of the conceptual risk profiling

The risk profile helps to estimate a possible vulnerability and warns the concerned security authority on future risks that the network or IoT devices can expose to an attack. The local repository at the IoT gateway is supported by a cloud system that provides an abundant resource in data storage and processing to the proposed security system. Three different risk sub-profiling is carried out considering contextual information, the outcome of the proposed intrusion recognition system, statistical attributes of IoT devices, and recent information about the third-party application running on it. The proposed conceptual risk profiling model also considers a profile manager powered with analytical and intelligent features to compute the final risk profile matrix table. The profile manager takes two inputs. The first one is the collection of sub-profiles in the form of a vector, and the second input is the enforced policy which is created by the security management team. The enforced policy has pre-defined attributes, provisioning schemes, risk scores, and weightage with which risk ranking are to be provisioned or de-provisioned. The risk profile matrix has rating the describes severity of the threat level as low, moderate, and high. A low rating indicator means that the impact of vulnerability or attacks will be minimal. A medium rating indicator indicates that the presence of vulnerability and the impact of the attacks may be destructive but can be restored if identified and resolved quickly. A high rating indicator represents that the impact could be significant and highly destructive. Based on the risk profile, a concerned entity or security administrator is able to assess current security levels, analyze the risks and vulnerabilities in the network and proactively respond to the changing parameters of the network before such risk and vulnerability come into any malicious action.

4. Results Analysis

This section discusses the outcome achieved and carries performance assessment of the proposed system with existing techniques. The design and implementation of the zero-trust security model are carried out on the numerical computing tool MatLab. The proposed work considers a case study of the enterprise IoT, where reliable communication and robust device security are of prime concern. In this regard, the discussion regarding the outcome is carried for both phases of security implementation. For the simulation purpose, the study considers the deployment of sensor nodes in the simulation boundary; however, the design of the proposed security scheme is carried out considering explicit characteristics of the IoT ecosystem.

4.1 Performance evaluation for network segmentation and secure communication

The description of the simulation parameters for the first phase of implementation is highlighted in Table 4. The evaluation of the first phase of the security approach is evaluated considering m throughput, end-to-end delay, and energy consumption. The scope and effectiveness of the proposed routing technique are justified based on the comparative analysis with existing solutions SEAR [30] and EOCER [31].

Table 4 description of simulation parameters

Simulation Parameters	Value
Simulation Boundary	100 m x 100 m
IoT devices	300
Packet Size	32 bits
Energy level	2joules
Control message	25 bits
Transmission range	10 meters
Simulation Round	50-500

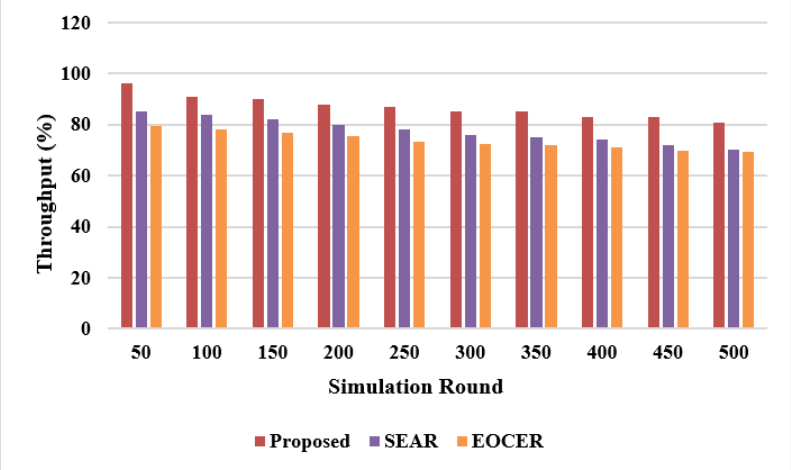

Fig.7 Throughput Analysis

The proposed system based on network segmentation and secure communication scheme outcome is compared with the existing scheme in terms of throughput is shown in figure 7. The graph's trend exhibits that the proposed scheme outperforms other existing schemes by achieving a better throughput score. Based on the closer analysis, it is observed that the proposed scheme made an average of 35% improvement in the throughput gain. This is because the proposed network segmentation scheme reduces the attack surface and enables distributed workload among IoT devices. Therefore, the possibility of overhead on single IoT devices is less, and this factor also leads towards achieving energy efficiency. Another potential factor of this phase of implementation is the lightweight and secure multipath routing approach, which enables the second line of defense in the IoT network and provides a reliable data transmission process. The existing techniques lack the reduction of attack surface in the network and do not have complete visibility of their devices. Therefore, it lacks comprehensive detection of network status and may forwards packet in the presence of an adversary. Another fact is that the proposed system has considered reducing energy consumption and security in every phase of network operation, which is missing in the existing system. The adversary can generate unnecessary route requests in the network to create heavy congestion.

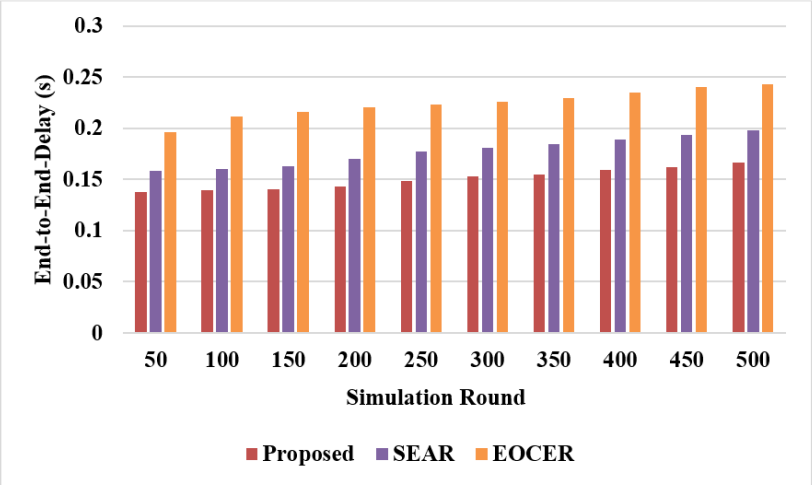

Fig 8 End to End delay Analysis

The performance evaluation of the proposed system is carried out in terms of end-to-end delay over increasing simulation round and compared with the existing scheme as shown in figure 8. The graph's trend exhibits that the proposed scheme outperforms other existing schemes with a significantly less end-to-end delay compared to existing solutions. The closer analysis of the graph trend exhibits that the proposed scheme has attained an average of 30% improvement in the delay reduction. The optimal multipath strategy for packet transmission based on the selection of intermediate data forwarder devices in different network regions makes the proposed system delay aware. This effective mechanism is missing in the existing solution. They are frequently used to select a longer route, which sometimes leads to re-transmission and lacks quantitative analysis to assess congested and faulty links, making existing solutions prone to threats.

Another interesting fact is that the proposed system introduces an effective and intelligent intrusion recognition system that offers real-time monitoring of network status and helps to maintain a risk profile that lets concerned security administrators take proactive action based on the analysis of risk profile. Moreover, based on risk profile,an effective strategy can be taken for network management in the proposed system.

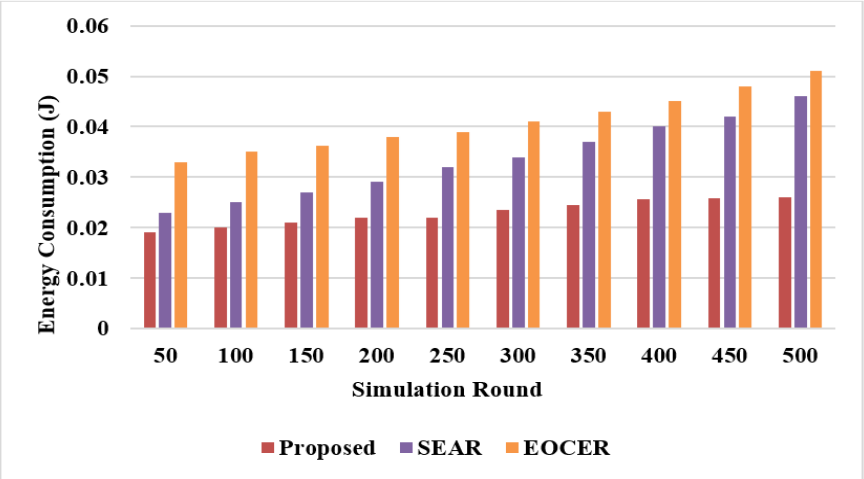

Fig 9 Energy consumption

The performance of the proposed system is evaluated and compared regarding energy consumption over increasing simulation round, as shown in figure 9. The graph's trend exhibits that the proposed scheme outperforms other existing schemes with significantly less energy consumption compared to existing solutions. The closer analysis of the graph trend exhibits that the proposed scheme outperforms existing solutions with an improvement of an average of 40% in energy savings. There are multiple reasons behind the performance of the proposed scheme. Firstly, the load on IoT devices is less during communication due to network segmentation. Secondly, formation of grouping based on the closer adjacent devices and assistance of data forwarder node in the packet transmission. Another interesting fact is that the proposed routing and data transmission is not associated with any unwilling factors of degrading communication performance. The lightweight design of the security key provides reliability in the packet transmission towards end-devices and awareness of network status and devices based on proposed IDS and risk profile. The main reason is that the nature of the proposed system is zero-trust, which means no trust-only assessment. Therefore, it carries a granular insight into network traffic and devices behavior using proposed LC-IRS. The proactive feature never allows an attacker to easily compromised any physical and virtual devices of the network. The next section discusses the performance of the proposed LC-IRS.

4.2 Performance evaluation of the proposed LC-IRS

In this section, the assessment of the proposed LC-IRS system is carried out and compared with other existing machine learning classification techniques. The study conducted a series of experiments by changing and adjusting the value of the proposed

model hyper parameters such as learning rate, epoch, and batch size to achieve the best outcome. Better performance has been observed when the learning rate is adjusted to 0.001. Different epochs 10,15, 20, 30, 50, and 100 are analyzed. It is found that the increasing number of epochs impacts the speed of learning rate, and finally, epochs are set to 20. Along with this, different batch sizes are also assessed with different values such as 256,512 and 1024. A significant performance gain is found with the large batch size; therefore, 1024 is selected to improve the model performance.

Table 5 presents performance analysis on different metrics for the proposed system and its comparison with different machine learning trained on the dataset. From the quantified outcome in table 4, it can be analyzed that the proposed LC-IRS outperforms other existing machine learning techniques concerning accuracy, recall, precision, and F1 score. However, random forest and decision tree exhibit similar performance. Decision Tree also achieved good performance in case of accuracy. However, SVM also exhibits good performance but not as proposed and other machine learning classifiers.

Table 5 Performance Analysis with different performance metrics

Evaluation	**Metrics**	**Comparison**			
		Proposed	**SVM**	**Random Forest**	**Decision Tree**
Training	Accuracy	99.5	96.09	98.3	99.02
	Precision	99	97	98	99
	Recall	99	97	98	99
	F1 Score	99	97	98	99
Testing	Accuracy	99.3	96.06	98.6	98.013
	Precision	99	96	98	98
	Recall	99	96	98	98
	F1 Score	99	96	98	98

Figure 10 and figure 11 exhibits a comparative analysis to assess the performance of the proposed system regarding accuracy (%) for both the training and testing phase with a different number of samples of the dataset.

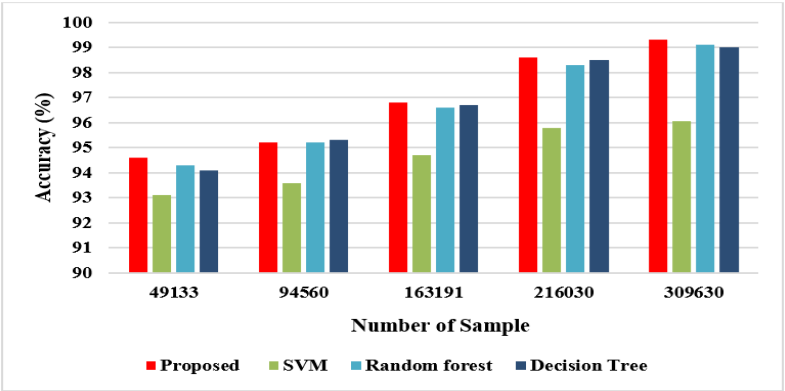

Fig 10 Training Accuracy

The graph trend analysis from figure 10 exhibits that the proposed system LC-IRS performed best in training in terms of accuracy over different dataset samples. However, the decision tree and ran forest both have shown approximately similar performance. It can also be observed that SVM has scored less accuracy score with linear performance on an increasing data sample.

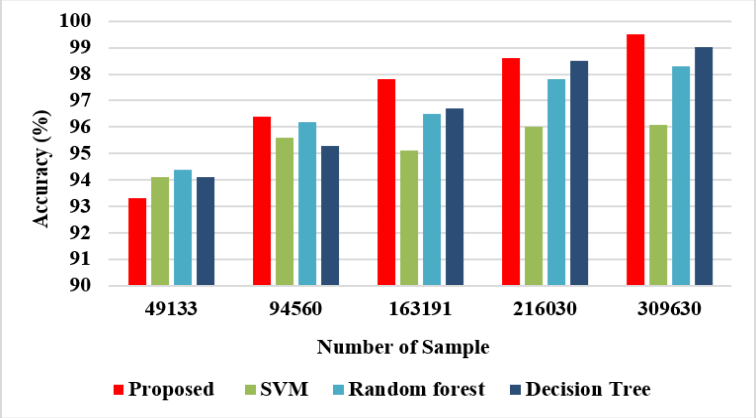

Fig 11 Testing Accuracy

The graph trend analysis from figure 10 exhibits that the proposed system LC-IRS performed best in testing phase different dataset samples. However, the proposed method initially exhibited a little less accuracy score when tested with 49133 number of dataset samples. Random forest exhibited a higher accuracy score, and both SVM and decision tree achieved similar performances. But for the rest cases of data samples, the proposed system outperforms other techniques, and the decision tree exhibits good performance.

5. Conclusion

The proposed research study considers a case scenario of an Enterprise Internet of Things (E-IoT) and focuses on IoT device security and data reliability. The prime objective of this study is to address the issues associated with a blind spot in the network and achieve a zero-trust security mechanism towards ensuring seamless communication and reliable data transmission in the critical applications of the enterprise. The entire contribution is proposed in multiple aspects. Initially, network modeling is carried out, where network segmentation and secure routing are introduced. This provides an effective mechanism that can discover a true knowledge network without ignoring any virtual and physical end-points segments of the network and prevent intrusion by lightweight cryptography XoR operation during data transmission. On the other hand, a lightweight and centralized intrusion recognition system (LC-IRS) is designed to perform real-time monitoring of network security status and detection of attacks. This phase of the module also maintains a reposit of their outcome to build a risk profile towards proactive defense in the network. The design of the proposed security model is

intended to achieve complete visibility of end-device connected to the network, granular insight on connected-device. The study implements real-time monitoring system to access device's function and behavior with other connected nodes and automatically classifies the vulnerable and threat risk associated with the IoT devices. The study outcome and performance analysis based on comparison justify the scopes of the proposed system in terms of efficiency, robustness, stability, and applicability to real-work applications.

References

[1] King, J., Awad, A.I. (2016). A distributed security mechanism for resource-constrained IoT devices. *Informatica (Slovenia), 40*(1), 133–143.

[2] Li, S., Xu, L.D., Zhao, S.(2015). The internet of things: a survey. *Inf Syst Front, 17,* 243–259

[3] Konur, S., Lan, Y., Thakker, D. (2021). Towards design and implementation of Industry 4.0 for food manufacturing. *Neural Comput & Applic*

[4] Park, D.S. (2018). Future computing with IoT and cloud computing. *J Supercomput* 74, 6401–6407

[5] Jayashree, L.S., and Selvakumar, G. (2020). Getting Started with Enterprise Internet of Things: Design Approaches and Software Architecture Models. Springer Nature.

[6] Khanna, A., and Kaur, S. (2020). Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications*, *114*, 1687-1762.

[7] "5G subscriptions to reach half a billion in 2022: Ericsson Mobility Report", https://www.ericsson.com/en/press-releases/1/2016/5g-subscriptions-to-reach-half-a-billion-in-2022-ericsson-mobility-report, Retrieved on 18 May 2021

[8] "IoT and OT Security Research Exposes Hidden Business Challenges", https://www.forescout.com/iot_forrester_study/, retrieved on 18 May 2021

[10] "What have we learned from WannaCry?", https://www.csoonline.com/article/3200673/what-have-we-learned-from-wannacry.html, retrieved on 18 May 2021

[11] "BlueBorne is Bluetooth's Stagefright moment", https://www.csoonline.com/article/3224447/blueborne-is-bluetooths-stagefright-moment.html, retrieved on 18 May 2021

[12] SonicWall cyber threat report. (2019). https://www.sonicwall.com. Accessed 18th May 2021.

[13] Fazal, K., Shehzad, H., Tasneem, A., Dawood, A., and Ahmed, Z.(2017). A Systematic Literature Review on the Security challenges of internet of things and their classification. *International Journal of Technology and Research,* 5, 40-48

[14] Aly, M., Khomh, F., Haoues, M., Quintero, A., and Yacout, S.(2019). Enforcing Security in Internet of Things Frameworks: A Systematic Literature Review. *Internet of Things*,100050

[15] Aljebry, D.F., and Tahir, S.(2017). Internet of things routing technique survey. *In Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 1-7

[16]Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84,* 25-37.

[17] Elrawy, M.F., Awad, A.I. and Hamed, H.F.(2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), pp.1-20.

[18] Mohammadi, V., Rahmani, A. M., Darwesh, A. M., and Sahafi, A.(2019). Trust-based recommendation systems in Internet of Things: a systematic literature review. *Human-centric Computing and Information Sciences,* 9, 21

[19] Bhandari, G. P., and Gupta, R.(2019). A systematic literature review in fault analysis for IoT. *International Journal of Web Science,* 3, 130-147
[20] Diro, A.A., Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of things. *Future Gen. Comput. Syst*. 82, 761–768.
[21] Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., Meshcheryakov, R. (2017). The cyber security in development of IoT embedded technologies, in: Proceedings of the International Conference on Information Science and Communications Technologies (ICISCT), 1–4.
[22] Anthi, E., Williams, L., Burnap, P.(2018). Pulse: an adaptive intrusion detection for the Internet of things, *Living in the Internet of Things: Cybersecurity of the IoT, 1-4*
[23] Kozik, R., Choras, M., Ficco, M., Palmieri, F.(2018). A scalable distributed machine learning approach for attack detection in edge computing environments. *J. Parallel Distrib. Comput,* 119, 18–26.
[24] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., and Lloret, J. (2017). Network traffic classifier with convolutional and recurrent neural networks for internet of things. *IEEE Access, 5, 18042-18050*
[25] Diro, A. A., Chilamkurti, N.(2018). "Distributed attack detection scheme using deep learning approach for internet of things," *Future Generation Computer Systems,* 82, 761–768
[26] Roy, B., Cheung, H.(2018). A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network. *28th International Telecommunication Networks and Applications Conference (ITNAC),* 1–6
[27] Soe, Y. N., Santosa, P. I., and Hartanto, R.(2019). Ddos attack detection based on simple ann with smote for iot environment. *Fourth International Conference on Informatics and Computing (ICIC),* pp. 1–5
[28] Cui, L., Yang, S., Chen, F.(2018). A survey on application of machine learning for Internet of Things. *Int. J. Mach. Learn. & Cyber.* 9, 1399–1417
[29] Koroniotis, N., Moustafa, N., Sitnikova, E., and Turnbull, B.(2018). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. *in eprint arXiv:1811.00701*
[30] Mu J., Liu X., Yi X.(2019). Simplified energy-balanced alternative-aware routing algorithm for wireless body area networks. *IEEE Access*, 7, 108295–303
[31] Kaur, N., Singh, S.(2017). Optimized cost effective and energy efficient routing protocol for wireless body area networks. *Ad Hoc Netw,* 61, 65–84