# Developing a Framework for Data Communication in a Wireless Network using Machine Learning Technique

Somya Khidir Mohmmed Ataelmanan [1]*, Mostafa Ahmed Hassan Ali[2]
Computer Science Department, College of Computer Engineering & Science
Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia[1]
Communication Engineering Departments, Faculty of Engineering, AL-Neelain University. Khartoum, Sudan[2]

***Abstract*—The emergence of Internet of Things (IoT) has become a huge innovation for utilizing the enormous power of wireless media. The adaptation of smart devices, with intelligent networking, has greatly enhanced the traffic of the IoT environment. The present security mechanism is primarily focusing on specific areas such as content filtering, monitoring techniques, and anomaly detection. A vulnerability reflects the inability of a network that allows an attacker to detect the extent of existing mechanism of security. The existing techniques focused on specific attacks rather than monitoring the whole network. However, there is a demand for a framework to govern and protect data and services in IoT network. Anomaly detection framework is a resource intensive activity to protect data and services of IoT / Wireless Sensor Networks (WSN). It supports application layer of IoT network and traces it frequently to find the existence of malicious activities. In this study, researchers proposed an anomaly detection framework to safeguard against wireless attacks. The proposed framework has employed a machine learning technique to detect the traces of wireless attacks. It supports IoT based networks to monitor the functionalities of the resources. In addition, it discusses the open challenges in IoT networks with possible solutions. Researchers employed a test bed for evaluating the proposed framework. The outcome of the study shows that the proposed framework provides better services with more security.**

***Keywords*—Anomaly detection; internet of things; wireless attacks; artificial intelligence; machine learning**

## I. INTRODUCTION

The technological developments in wireless communications and Artificial Intelligence (AI) technologies have enabled the design of WSNs, where sensor nodes capture and exchange intelligible data from their surrounding environments in a wireless form and transfer it to the proper destination. According to scientific publications, the total wireless sensor numbers used are projected to exceed 60 trillion at the end of 2022, representing 10,000 wireless sensors for each person worldwide [1]. Thus, all the WSN's problems and challenges will expose the researchers to abundant topics. WSNs have begun to draw interest in academics due to wireless technology and embedded electronics due to wireless technology's rapid technological growth [2]. A typical WSN consists of small devices known as nodes. These nodes are embedded CPUs, minimal CPU power, and smart sensors. WSNs are one of the most promising innovations for the third millennium and have a broad range of applications globally. WSNs in different applications are commonly used because they have enormously attractive features such as low manufacturing costs, low installation costs, unattended network operations, autonomous operation and long service life [3]. By introducing Internet connectivity potential into sensor nodes and sensing abilities on internet-connected devices, WSNs began blending to the Internet of Things (IoT) [4]. IT will be incorporated into IoT during this time, and countless Sensor Nodes enter the Internet to co-operate with other nodes in order to sense and manage their environment. IoT revolutionizes the IT field and will be the next significant technological leap after the Internet. In the near future, IoT will provide connectivity between people and the world through the WSNs.[5] The WSN will provide IoT with Internet access to an immense quantity of data obtained from the WSNs. Therefore, IoT's safety should begin with securing WSNs before the other components in the first place. The IoT market is anticipated to increase to more than 75 billion in 2025 by over 15 billion devices in 2015[5]. It means on average that every human on Earth has a minimum of 25 IoT devices per person. It is now predicted that IoT will have a significant effect on our lives soon [6]. However, due to the absence of a physical line of defence, i.e. no dedicated infrastructure like gateways for detecting and controlling information flow in the network, security for WSNs and IoT is essential to the scientific community[8][9]. In particular, WSNs and emerging IoT technology can be an open route for attackers in the application domains, where the CIA (confidentiality, honesty, and availability) is primarily relevant. In addition, new integration and joint work between WSNs and IoT would open up new opportunities and security challenges. Regarding scalability, it is often challenging to implement IoT applications, which involve a large number of devices as time, memory, processing and energy constraints are limited [10]. For instance, calculating regular temperature changes across the country could require millions of devices and result in unmanageable data. Furthermore, the hardware used in IoT does have various operational features, such as sampling rates and error distributions, whereas IoT sensors and actuators are often too complex. All these factors are responsible for building up a heterogeneous IoT network in which IoT data are deeply heterogeneous. In addition, it costs a large amount of raw data to be distributed across the diverse and heterogeneous network. IoT requires compression of data and data fusion to

*Corresponding Author

minimize the data volume. Therefore, it is desired to standardize the understanding of data care for future IoT. Furthermore, hackers, malware and viruses could disrupt data and information in the communication process. IoT is also commonly used in social life applications, such as smart grid, smart transportation and smart home [11]. IoT also contains access cards, bus cards and some other small apps. IoT software can make people more convenient, but private details can be leaked anytime if it cannot provide personal privacy protection. Once the IoT signal is stolen or disrupted, the entire IoT information's security is directly affected. The widespread IoT provides more information and will raise the risk of exposure to such information. On the one hand, IoT does not have the right security solution on the other hand, its innovations would be mostly limited.

WSN and IoT safety is an important problem, especially if commissioned with mission-critical tasks; for example, when a network safety gap leads to casualties for friendly forces on a battlefield in military tactic applications. A recent paper [12] revealed that the majority of the systems currently used fail to embed strong security services which can protect the privacy of patients. None of the patients would be glad if their sensitive health details were exposed to misbehaving nodes and system failures by leakage. The WSN secure algorithms and methodologies shall be applicable for any IoT consisting of one or more sensor networks. As previously reported, WSNs will most likely be implemented in the near future with IoT [13][14]. All cybersecurity problems, in particular attacks, prevention and mitigation are therefore very necessary to create a safe and secure IoT. WSNs are vulnerable to a number of attack methods that could pose essential security threats. These attacks may be linked to two major categories: active and passive [15][16]. In the category of passive attacks, attackers normally are disguised (camouflaged) and either damage the network components or use the connection to gather useful information. Passive attacks can also be classified into types of eavesdropping, disruption of nodes, malfunction of the node, node interrupt and monitoring of traffic. Whereas an attacker affects the roles and activities of the target network in the active attacks group [17][18]. The effect can be the actual target of the intruder and can also be identified by means of protection mechanisms (intrusion detection). For example, as a result of such attacks, network services can be interrupted. Flooding, Denial-of-Service (DoS), Blackhole, Wormhole, Sinkhole and Sybil types are some of the active attacks [19][20][21]. IoT security covers a range of areas, for example, attacks and countermeasures, protection, confidence, key distribution, patch management and access control. Therefore, IoT nodes can be managed via the Internet and sent sensed data (or sensed information data) to internet-based data sinks [21]. Today, IoT networks can also involve or communicate with new concepts like Big Data and Cloud/Configuration, etc.

The objective of the research is as follows:

- To propose an anomaly detection framework for IoT / WSN.
- To develop an interface to monitor the IoT / WSN environment using a machine learning technique.
- To suggest some possible solutions for open challenges in IoT / WSN.

The proposed framework supports IoT based networks to govern the resources and identify the anomalies. In addition, it overcomes the challenges in the existing framework. The existing techniques consider only a specific attack in the wireless network. The emergence of modern technologies leads to the development of new attacks in IoT network. Therefore, there is a demand for effective framework that can adapt to a newer environment and able to detect untraced anomalies.

The remaining part of the paper is structured as follows: Section 1 summarizes the concept of WSN, IoT with its security limitations, effects and future predictions, while Section 2 introduces different types of WSN and IoT attacks. Section 3 provides the proposed framework for secured IoT communications. The outcome of the study is presented in section 4. Section 5 discusses the open challenges and policies for monitoring IoT network. Finally, section 6 concludes the research with its future direction.

## II. Research Background and Realted Works

WSNs are node arrays, and those nodes are computerized systems, respectively. These sensors usually work together to create centralized network systems [1] [2]. There are some criteria for using nodes such as reliability, multifunctionality and wireless use of these networks. In addition, each node in every network has a defined purpose. For example, if it is intended to gather microclimate information in a densely populated area, the nodes are positioned on a network of buildings or residential area throughout the specific region. In this network, the system for communication and data sharing should be centrally structured and synchronized. IoT not only has security threats similar to sensor networks, mobile communications and Internet however also specializes such like privacy issues, different network configuration authentication and access control issues, storage and administration of information, etc. One of IoT's application challenges is data and privacy security [3]. In IoT, RFID systems, WSN sensor systems are aware of the end of information technology which, with the password encryption technology, protects the integrity and confidentiality of information [7–9]. Many forms of encryption of data and information are available, including random hash lock protocol (hash function), hash chain protocol, infinite channel extract key, Encrypted ID, and so on [11-12]. Authentication of identity and access control can decide the correspondence between the two parties and reiterate each other's true identity, prevent covert attacks to ensure the authenticity, validity of data, and so on [15–17]. The transmission method has two significant security problems. One of the risks is the IoT security, and the other is the related network construction and implementation technology [15]. It should deal with the incompatibilities between various networks that are vulnerable to problems of protection, for instance, it is difficult to create the interconnection between the relationship as the relationship of trust among nodes are constantly changing; however, this can be solved through key management and protocol routing [18-20]. Security issues like DOS/DDOS attacks, forgery/middle attacks, heterogeneous network attacks, ipv6

application risk, and conflicts with the WLAN application also affect IoT's transport security [18][21]. Due to the huge volume of data, it is possible to create network congestion in the core network. The capability and connectivity problems such as space management, redundancy and security requirements in the reference framework should be taken into full account [21]. The security issues of application include access to and user authentication, the privacy of information, data stream destruction, reliability of the IoT network, middleware security, management platform, etc. To ensure technology protection and improve the aspect of basic safety and expectations of human behaviour, IoT usage is strongly tied to contemporary societies. In the meantime, research has also been carried out on people involved in CPS (cyber-physical systems) and overall computer protection. Sensitive IoT layers include Perception layer, transport layer and application layer. Hacker makes all IoT devices vulnerable in the network due to the limited handling capacity of IoT devices because they seemed to have a stronger signal than the actual access point with the same identificatory as the IoT service package. This allowed all network communications to be compromised to eavesdropping and Man in the Middle (MiM) attacks [21]. These scenarios for attacks have created a situation in which IDSs can be used in IoT networks to discover IoT devices vulnerabilities. The concept of IoT focuses on the intelligent incorporation of a specific physical world with the Internet in order to promote interaction; for this purpose, interconnections and dependencies in IoT environments with a number of heterogeneous environments. Any IoT device is therefore exposed to cyber threats in any related environment. Although IOT security threats can be divided widely into cyber- and physical realms, our survey is primarily concerned with cyber-threats, both active and passive attacks. IoT-based environments are subject to a range of physical and virtual dimensions of threat. Passive attacks are distinguished by a lack of changes in data or its flow, thus only affecting communications confidentiality and privacy. Passive attacks in some cases can allow IoT devices to be tracked locally. Active attacks include active change, alteration, and flow of information, but not limited to system settings, software and control messages. The IoT framework is used as a vector to launch large DDoS against Internet networks, and is also an aggressive attack. Since their large number and comparative ease of compromise, poor security standards and weak protection mechanisms, IoT systems are an effective vector for such attacks. Fig. 1 illustrates the user interface and network service attacks on IoT environment.

Most IoT systems use a certain kind of user interface to provide services to users via IoT systems (mobile, desktop or web application). The customer can monitor the case of smart home appliances through mobile applications. The rapid growth of smartphones has provided malicious entities with malware as innocuous mobile apps that they can publish without detection through applications. Often smartphones can also be hacked by bugs in platforms such as Android vulnerabilities. This results in exposure of malware compromise to all information that is stored on the telephone. The attacks allowed by user interface platforms include eavesdropping, location monitoring, DoS/DDoS, and bluejacking.

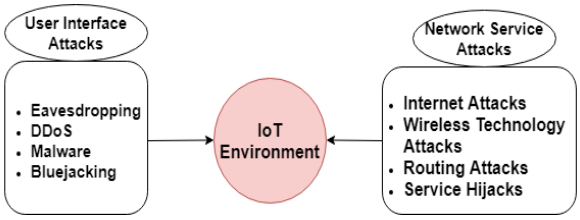


Fig. 1. IoT Attacks.

Network service attacks refer to the attacks targeted to the network configuration of IoT devices[6]. For instance, hackers target IoT devices configuration parameters in order to compromise the device and gain access. Wireless technology attacks are becoming familiar due to the emergence of sophisticated hacking tools. Using these kinds of tools, the IoT network can be hacked by the hackers. Internet and routing attacks means the unauthorized access of protocols of a network whereas the service hijacks indicate the unauthenticated usage of functionalities of IoT devices.

Based on the research background, researchers raised the following Research Questions (RQ).

RQ1 – How to detect anomalies in WSN / IoT network?

RQ2 – How to apply Machine Learning (ML) techniques to prevent attack in data communication in WSN / IoT environment?

RQ3 – What are the criteria for evaluating the performance of anomaly detection methods?

To present a solution for RQ1, authors performed a systematic literature review on methods that detects anomalies in IoT network using ML approaches. The following part of this section will present the outcome of the review.

Abhishek Verma and Virender Ranga[1] developed a ML based approach for detecting anomalies in IoT network.They explored the capability of classification algorithms for machine learning in order to protect IoT against DoS attacks. A systematic study is conducted on classifiers that can further improve intrusion detection systems based on anomalies (IDSs). Classifier performance evaluation is carried out by using familiar evaluation and validation techniques. They employed common datasets such as CIDDS-001, UNSW-NB15, and NSL-KDD.

Authors [2] developed an approach to cyber security, deep learning, to detect attacks in social IoT. The efficiency of the deep model compared to conventional machine learning approaches is evaluated by a distributed attack detection system. The distributed attack detection system had shown to be superior to the centralized detection systems of a deep learning model. It was also shown that the deep model is more efficacious than its shallow counterparts in attack detection.

Authors in [3] considered the integration of the collection of functions, cross validation and classification of the domain, which has not been taken careful into account in current literature. The outcome of this study with recent attacks dataset indicates that the method was capable of effectively detecting cyberattacks. It can detect infected IoT devices that pose a significant challenge in the cloud computing context. The

technique was based on the implementation of a model of training in the distributed fog networks, which can intelligently learn from IoT devices and detect attack or anomaly.

In [4], authors investigated the possibility of using anomaly detection methods based on master learning in vertical wall systems, to boost automation and intelligence in order to achieve predictive climate maintenance. Two types of abnormalities are studied, namely point anomalies and contextual abnormalities. Method of indoor climate anomaly detection, based on forecasts and patterns of recognition were investigated and applied. The results show that in terms of detection points and contextually abnormalities, neural network models, especially the auto encoder (AE), and the long term memory decoder (LSTM-ED), can therefore be deployed to industrial systems in vertical power walls. The results propose a new method of data cleaning and a prediction method is in practice implemented as a proof of concept in the cloud. This study shows the developments in the learning of machinery and the Internet of things that can be completely used to speed up the solution growth.

Authors in [5] discussed different types of attacks and anomalies were suggested and explored in this research based on an intrusion detection method in the IoT. Authors have used the CICIDS data set to detect attacks while assessing the performance of the proposed deep-learning model DBN-IDS framework. Various attacks with several labels and numbers of attacks were presented in this data set. The attack types present in this dataset were DoS/DDoS, Botnet, Brute Force, Web Attack, Invasion, and PortScan, which could cause IoT device failures. They proposed a dedicated, knowledge-based Deep Belief Network (DBN) intrusion detecting system algorithm model in this work. The CICIDS 2017 dataset was used for the performance analysis of their IDS model in relation to attacks and anomaly detection. In all the parameters for accuracy, precision, F1-score, and detection rate, the proposed process generated better performance.

In [6], the author explored similarities between several widely used Support Vector Machine (SVM) classifiers and several other ensemble algorithms, namely, LADTree, REPTree, Random Forest (RF) and MultiBoost, on the other hand. The study was based on a variety of Weka testing methods with the goal of estimating and comparing a selected performance metrics. The results obtained indicate that RF algorithm can be classified as reliable, whereas the REPTree algorithm is the alternative recommendation in the more restrictive timeline cases.

Authors in [7] introduced an ensemble approach that uses the Deep Neural Network (DNN) and LSTM as well as a meta-classifier using the stacking generalization principle. The method used a two-stage approach for the evaluation of network anomalies, with a Deep Sparse AutoEncoder (DSAE) in the first phase, to improve the capabilities of the proposed approach. In the second step, a classification technique was used to stack ensemble learning. The findings of an assessment of the strategy proposed were discussed. The statistical value of network anomaly detection was checked and compared to state-of- the-art approaches. Table I illustrates the features and limitations of the existing literature.

TABLE I. FEATURES AND LIMITATIONS

| S.No. | Authors | Features | Limitations |
|---|---|---|---|
| 1 | Abhishek Verma and Virender Ranga [1] | Application of classification algorithms to predict DoS attacks. | Only Dos attacks were discussed. Authors focussed on the classification of attacks rather than detecting attacks. |
| 2 | Diro, A. A., & Chilamkurti, N. [2] | Developed a distributed attack prevention technique based on deep learning approach | The detection speed of the approach was less rather than the learning speed. |
| 3 | Md Mamunur Rashid et al. [3] | Suggested a classification algorithm to detect anomalies in IoT devices in fog computing | The focus of the study was on fog computing. Authors employed multiple types of attacks dataset, however, partially related to IoT devices. |
| 4 | Yu Liu et al. [4] | Developed a method to detect anomalies in IoT environment. Authors applied LSTM to identify anomalies in IoT networks. | Authors employed limited set of data for evaluating their methods. In addition, they failed to discuss the network performance during the anomaly detection. |
| 5 | Manimurugan S et al. [5] | Proposed a DBN based IDS in IoT network. | Authors evaluated the system with a limited set of attacks. No discussion about network performance. |
| 6 | Valentina Timčenko and Slavko Gajin [6] | Addressed different kinds of classifiers and its performance on identifying various kinds of IoT attacks. | Authors argued that the performance of RF classifier was better than another classifier. However, they evaluated the classifiers with limited dataset. |
| 7 | Vibekananda Dutta et [7] | Authors proposed a LSTM based DNN for identifying IoT attacks. | Multiple datasets were employed for measuring the performance of the IoT detectors. However, authors failed to discuss the network performance of IoT environment. |

Based on the outcome of the literature review, researchers selected Yu Liu et al. [4], Vibekananda Dutta et al. [7]. Comparing to the recent studies, the performance of the selected works is better. Both studies employed LSTM as a technique to identify an attack in IoT network.

## III. RESEARCH METHODOLOGY

In this study, the researcher proposed a framework that provides a secure wireless network environment, especially IoT devices. Fig. 2 presents the proposed framework for transmitting data among IoT devices. RQ2 stated that how ML technique can improve the performance of detector to identify / classify attacks in IoT environment. To provide a solution, authors presented studies that addressed the limitations of the wireless networks. Basically, IoT devices operate on top of the

physical layer of wireless networks. The introduction of malicious devices among the existing devices can damage the whole network. In the word "recurring neural network" two large network groups are considered to consist of a similar general structure, one of which is a finite input and the other an infinite input. Both network classes have complexities over time. A repetitive finite impulse is a directed acyclic graph that can roll down and be replaced by a neural network strictly supplied, while a repeating network of endless impulses is a cyclically driven graph that cannot roll down. Long Short-Term Memory (LSTM) is one of the variations of RNN. It contains a dedicated memory to produce an output based on the previous events. The efficiency of LSTM is improved with multiple gates. LSTM eliminates back propagation in contrast to RNN. Each LSTM input produces an output which becomes an input for the next LSTM layer or module. And when major events are delayed over long periods, it can accommodate signals that combine low and high-frequency components. In the proposed framework, the researcher introduced an intelligent interface that governs an IoT network. The development of interface is based on AI-based approach. LSTM in Fig. 2 is applied to identify a malicious node in the network. The researchers employed a supervised learning technique to train the NB classifier, which indicates the vulnerability as a label. They developed a testbed for evaluating the proposed framework.

LSTM models are extremely powerful in handling complex data. It contains five components that allow producing both short - term and long - term data.

Cell state (C) - It indicates the intrinsic memory.

Hidden state (H) - It represents an output state information based on the current input, hidden state, and current cell input.

Input gate (I) - It is used to decide the total number of data that can be passed to the cell state.

Forget gate (F) - It decides the total number of data that can be transferred from current input and previous hidden state to the present cell state.

Output gate (O) - It indicates the total number of data that can be passed from the current cell state to the hidden state.

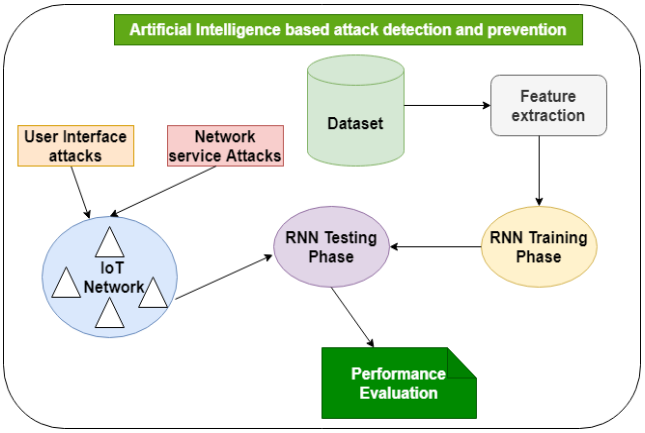


Fig. 2. Proposed Framework for IoT Networks.

### A. Input Gate

It figures out which input value for memory modification should be used. The values up to 0,1 are defined by Sigmoid. And the tanh feature tests the transmitted values and assesses their importance from-1 to 1. The input gate and cell status are represented by Equation 1 and 2.Wtn is the weight, $H_{t-1}$ is prior state to the hidden state, $x_t$ is an input, and $b_n$ *is the bias vector* that requires for learning rate in the training phase. The cell state is calculated through tanh function.

$$I = \partial(Wt_n(H_{t-1}, x_t) + b_n) \quad (1)$$

$$C = \tanh(W_d(H_{t-1}, x_t) + b_c) \quad (2)$$

### B. Forget Gate

It identifies and discards the block information. The sigmoid function is used to define the forget gate for LSTM. Equation 3includes ( $HT_{t-1}$ ) and input ( $x_t$ ) that are examinedand the number of outputs among 0 and 1 is verified by each cell state $C_{t-1}$ number.

$$F = \partial(Wt_f(H_{t-1}, x_t) + b_f) \quad (3)$$

### C. Output Gate

For deciding the outcome, the input and the memory of the block are used. Sigmoid defines the values to move between 0 and 1. The tanh function weights the values transferred, which are determined in their value from -1 to 1 and multiplied by Sigmoid efficiency. Equation 4 and 5 represents the output gate and hidden gate to identify an attack in IoT network.

$$O = \partial(Wt_o(H_{t-1}, x_t) + b_o) \quad (4)$$

$$H = O_t * \tanh(C_t) \quad (5)$$

Researchers employed IoT attacks dataset [8] to evaluate the performance of the proposed framework. The study focussed to protect IoT network from application and network layer attacks. Authors developed the framework using anomaly-based detection. A testbed is utilized with 10 IoT devices with a ML based interface. Authors applied Long Short-Term Memory (LSTM) version of RNN to train the model to detect the anomalous traces in the network and IoT configuration parameters. Multiple types of attacks such as DDoS, Key Logging, etc., are analysed and traces are utilized as a label for training RNN_LSTM.

Algorithm 1 presents the data collection processes for IoT attacks detection. Authors intended to develop ML based technique. Researchers employed IoTID20 dataset [8] to train and test the performance of the proposed method. Apart from this dataset, they developed a multiple attack anomaly and applied in the test bed.

Algorithm 1 Data Pre-Process

Input: IoTID20, GenID21

Output: Vectors

1: Procedure Data Pre- Process
2: while i <- item do
3: D <- RemoveIrrelevant(i)
4: D1 <- RemoveSpacesInString(D)
5: D2 <- TransformAsVector(D1)
6: end while
7: return D2
8: end Procedure

Algorithm 2 presents the training phase of anomaly detection in IoT networks. The extracted vectors are treated as an input for training phase and attacks are produced as an output. The LSTMfeed function stores the attack parameters as features and support proposed method (LSTMAD) to identify an attack.

Algorithm 2 Training - Anomaly Detection

Input: IoTID20, GenID20- (Vectors)

Output: User Interface / Network Service Attack

1: procedure Training phase (vector)
2: while vector <- Vector do
3: if vector = Feature(IoTID20 / GenID20) then
4: attack = Network Service / User Interface Attack found
5: else
6: attack = No Attack
7: if attack = LSTMfeed(feature) then
8: attack = Network Service / User Interface Attack found
9: else
10: attack = No Attack
11: end if
12: end if
13: end while
14: return attack
15: end procedure

Algorithm 3 shows the testing phase of LSTMAD which monitors the data communication in the IoT network and identity anomalies in the network. It verifies the device configuration parameters in the network and predicts user interface and network service attacks. Throughput and control overhead criteria show the performance of the network. Thus, these conditions justify the overall performance of the IoT attack detectors. During the testing phase, LSTMAD monitors the IoT network in a specified interval of time during the communication of data among IoT devices.

Algorithm 3 Testing Phase - Anomaly Detection

Input: Transmission of data in vulnerable environment

Output: Type of URL

1: Procedure Testing phase
2: while D <- Data do
3: if element <- LSTMMemory = Feature (Device configuration / User Interface parameters) then
4: attack = Network Service / User Interface Attack found
5: else
6: attack = No Attack
7: feedback = Environment (suspicious)
8: if element <- LSTMMemory = f<- feedback then
9: attack = Network Service / User Interface Attack found
10: else
11: attack = No Attack
12: end if
13: end if
14: Throughput = Number of packet received / Total time
15: Network overhead = Number of control overheads / Number of received packets
16: end while
17: return attack
18: end procedure

Fig. 3 shows the snippets of learning rate to train the IoT attack detectors. Epoch means the frequencies to monitor the IoT network. Both IoTID20 and GenID20 are used in this study to train and test the detectors. IoTID20 contains 625380 attack parameters that represent network service and user interface attacks. In addition, authors generated 23000 attack parameters related to the recent IoT attacks.

```
for IoT_epoch in IoT_range(no_of_epochs):
  new_IoTlr_decay = orig_IoTlr_decay ** max(epoch + 1 - max__epoch, 0.0)
  attack.assign_lr(sess, learning_rate * new_IoTlr_decay)
  current_state = nump.zeros((num_layers, 2, batch_size, attack.hidden_size))
  for step in range(training_input.IoT_epoch_size):
    if num % 75 != 0:
      cost, _, current_state = sess.run([attack.cost, attack.train_op, attack.state],
                                        feed_dict={attack.init_state: current_state})
    else:
      cost, _, current_state, acc = sess.run([attack.cost, attack.train_op, attack.state, attack.accuracy],
                                             feed_dict={attack.init_state: current_state})
      print("Epoch {}, accuracy: {:.3f}".format(epoch, step, cost, acc))
```

Fig. 3. Snippets – Training Epoch.

## IV. Results and Discussions

In Python 3.0 with support from Sci - Kit Learn and the NUMPY packages, the proposed method (LSTMAD) is developed. In addition, the existing IoT attack detectors are designed for evaluating the efficiency of LSTMAD. The settings for the method parameters during training and test phases are shown in Table II. The learning rate, epoch limit, lot size and decay are the parameters to tell the methods to carry out the results many times. Vocabulary and threshold values are important parameters for the test stage to achieve results through the test dataset.

Authors selected a recent dataset that contains 64.2 million attacks relevant IoT attack in order to answer RQ3. Criteria such as learning rate, accuracy, F1 – Score, Throughput and Control overhead are applied to evaluate the performance of methods. IoT attack detectors are evaluated with a testbed that contains 10 number of IoT devices. Table III presents the learning rate of detectors with IoTID20. The learning rate is increased from 1.0 to 5.0 and number of attacks learnt by each detector is measured. LSTMAD has achieved 93.6 percent of attacks with learning rate of 5.0 whereas Yu Liu et al. [4], and Vibekananda Dutta et al. [7] have achieved 91.5% and 92.4 %, respectively. LSTM is the base technique for all detectors which made detectors to achieve better learning ability. Table IV shows the learning capability of detectors with GenID20 dataset. The dataset contains limited number of attacks rather than IoTID20. Thus, the learning rate of detectors is higher and similar to each other.

Fig. 4 represents the throughput of IoT network. A set of data is communicated between IoT devices in the simulated network. It is evident from the figure that the throughput of the IoT network with LSTMAD is better comparing to Yu Liu et al. [4], and Vibekananda Dutta et al. [7] Throughput is measured in multiple time period with different set of data.

TABLE II. Initial Settings of Parameters (Training and Testing Phases)

| Methods | Training phase | Testing phase |
|---|---|---|
| LSTMAD | learning_rate=1.0, max_lr_epoch=9, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data | batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2 |
| Yu Liu et al. [4] | learning_rate=1.0, max_lr_epoch=9, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data | batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2 |
| Vibekananda Dutta et [7] | learning_rate=1.0, max_lr_epoch=11, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data | batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2 |

TABLE III. Learning Rate – IoTID20

| Learning Rate | LSTMAD | Yu Liu et al. [4], | Vibekananda Dutta et al. [7] |
|---|---|---|---|
| 1.0 | *87.6* | 89.7 | 86.4 |
| 2.0 | *88.4* | 88.4 | 85.6 |
| 3.0 | *91.6* | 90.7 | 89.6 |
| 4.0 | *92.4* | 90.9 | 90.8 |
| 5.0 | *93.6* | 91.5 | 92.4 |

TABLE IV. Learning Rate – GenID20 Dataset

| Learning Rate | LSTMAD | Yu Liu et al. [4], | Vibekananda Dutta et al. [7] |
|---|---|---|---|
| 1.0 | *94.7* | 90.5 | 89.6 |
| 2.0 | *96.8* | 91.6 | 84.9 |
| 3.0 | *97.5* | 90.8 | 90.7 |
| 4.0 | *98.6* | 90.1 | 89.7 |
| 5.0 | *98.3* | 91.4 | 91.3 |

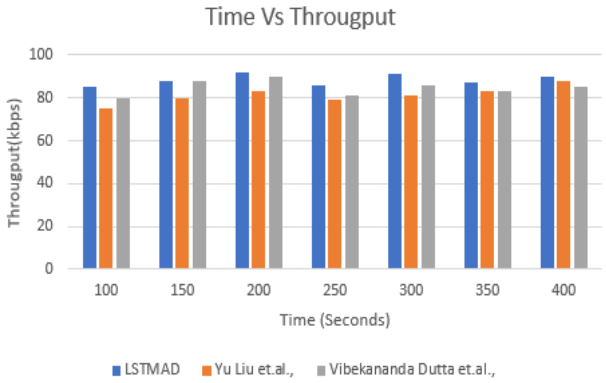


Fig. 4. IoT Network Throughput.

Fig. 5 illustrates the control overhead of IoT network with IoT attack detectors. The control overhead represents the excessive data added with normal data during the communication. The proposed detector required less overhead to govern transmission of data in IoT network. In 400 seconds, the method of Vibekananda Dutta et al. [7] required more than 16000 Bytes of overhead to monitor the network whereas LSTMAD needed only 12000 Bytes of control overhead.

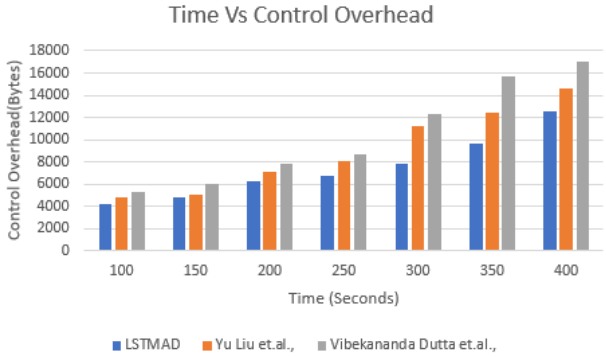


Fig. 5. Control Overhead of IoT Network.

Table V includes the accuracy of each IoT detectors with IoTID20 and GenID20. Accuracy of proposed IoT attack detector is 95.6 % in 450 seconds for IoTID20 dataset whereas Yu Liu et al. [4] and Vibekananda Dutta et al. [7], have achieved 93.8% and 94.6 % in 430 and 520 seconds, respectively. Fig. 6 and Fig. 7 shows the relevant figure of Table V. For GenID20 dataset, LSTMAD has achieved a superior accuracy of 96.3% in 246 seconds which is better than other two detectors.

TABLE V. ACCURACY OF DETECTORS

| Methods | IoTID20 | | GenID20 | |
|---|---|---|---|---|
| | Accuracy (%) | Time (in Seconds) | Accuracy (%) | Time (in Seconds) |
| LSTMAD | *95.6* | *450* | *96.3* | *246* |
| Yu Liu et al. [4] | 93.8 | 430 | 94.8 | 301 |
| Vibekananda Dutta et [7] | 94.6 | 520 | 93.1 | 432 |

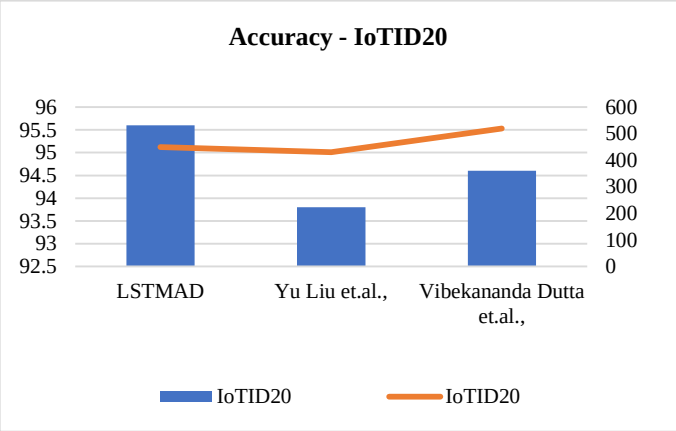


Fig. 6. Accuracy of IoTID20.

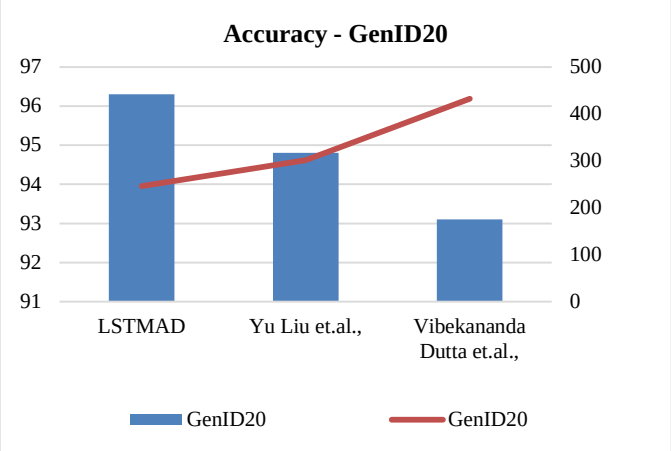


Fig. 7. Accuracy of GenID20.

Table VI presents the F1 – Score of detectors for IoTID20 and GenID20 datasets. F1 – Score represents the retrieving capability of detectors. The retrieving capacity of LSTMAD for IoTID20 is better than Yu Liu et al [4], and Vibekananda Dutta et al. [7]. The performance of LSTMAD on GenID20 dataset is similar to other methods; however, consumes less amount of time. Fig. 8 and Fig. 9 illustrate the performance of IoT attack detectors. Data pre-process activity of this study supports the classifying process to achieve effective results rather than the other detectors. In addition, it requires limited number of data that improves the throughput of IoT network.

TABLE VI. F1 – SCORE OF DETECTORS

| Methods | IoTID20 | | GenID20 | |
|---|---|---|---|---|
| | F1-Score | Time (in Seconds) | F1 – Score | Time (in Seconds) |
| LSTMAD | *93.4* | *450* | *91.8* | *246* |
| Yu Liu et al. [4] | 90.1 | 430 | 93.2 | 301 |
| Vibekananda Dutta et [7] | 89.4 | 520 | 91.6 | 432 |

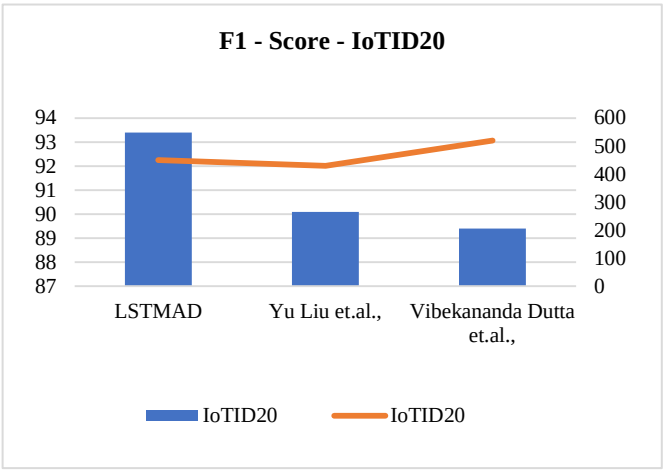


Fig. 8. F1 – Score of IoTID20.

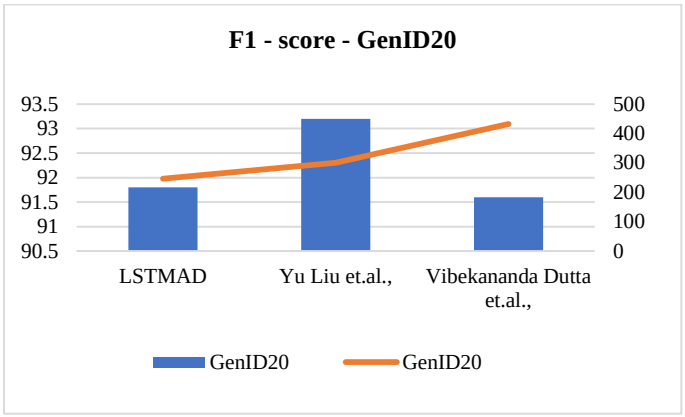


Fig. 9. F1 – Score of GenID20.

## V. OPEN CHALLENGES AND POLICIES

The growing impact of IoT security on the Internet and its users is essential to protect the future of the Internet. In order to protect against Internet threats, IoT-based attacks, IoT manufacturers, IoT service providers, users, SDOs, policy makers and regulators will all be ordered to carry steps. The influence that IoT security has on the trust and online use of

users is also important to understand. Trust is a key component of a sustainable, evolving, global Internet. Users feel vulnerable and excluded without trust and reluctant to take advantage of the many legitimate benefits offered by the Internet. The following part of this section will provide some open challenges and policy requirements for maintaining IoT networks.

### A. Challenges

A collaborative security approach [11] is essential for the challenges posed by IoT as much as ever. If the IoT Ecosystem expands, the number of connected devices that can be vulnerable may increase. These systems must not be vulnerable. While each actor is responsible for their own tasks, we together need to take steps to reduce the risk that we can generate vulnerable equipment, while reducing the effect of vulnerable devices as they find their way on the network [1][3].This paper is directed at regulators, policymakers and everyone who is involved in developing and implementing IoT security policy tools.

*1) Weak security:* Competitive pressures for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems, including devices, applications and services, to devote less time and resources to security[6][7]. Strong security can be expensive to design and implement, and it lengthens the time it takes to get a product to market. The commercial value of user data also means that there is an incentive to hoard as much data for as long as possible, which runs counter to good data security practices [9]. Additionally, there is currently a shortage of credible and well-known ways for suppliers to signal their level of security to consumers.

*2) Complex system:* The system's security is as strong as its weakest link. In IoT systems, various components can be operated by different parties in different jurisdictions (for instance, a server in one country may be located and a system may be produced in another country and used in another country), making it difficult to cooperate in the resolution of security issues in IoT and raising problems with cross-border compliance [11]. Complex supply chains challenge security assessments, which require networks to be holistically secured and organized between various parties and parts of the system. IoT systems are increasingly operated and/or controlled by remotely managed cloud providers (or at least strongly interacting with them) rather than being controlled locally. There may also be a specific issue of lack of accountability and control for the end-user.

*3) Limited knowledge:* Consumer knowledge of IoT Protection is limited and affects their safety factor in their shopping habits or the configuration and safeguarding of their IoT Systems [2]. Consumer groups also face financial limitations that make it especially difficult for customers to interact and learn.

*4) Legal liabilities:* It may be difficult to assess the responsibility for damage due to insufficient IoT protection. In order for victims to assign liability or get compensation for harm, this results in uncertainties. Clear liability may serve as an opportunity to improve protection [5]. Ultimately, in the absence of strong liability regimes, consumers pay for safety violations.

### B. Policies and Guidelines

Policies to protect from threats to the web infrastructure, such as IoT-based DDoS attacks are all required [17]. The effects that IoT protection has on user trust and online application should also be understood. Trust is a critical element for a sustainable, changing and global Internet. Without trust, users are helpless and oppressed and reject the many valid advantages of the internet.

*1) Data protection:* Data gathered or used by IoT should be protected by privacy and data protection laws, especially the sensor data [18]. Governments will enhance security and safety by clarifying how IoT applies current regulations on the protection of privacy, data protection and consumer protection. In addition, businesses should not make false or disappointing claims about the safety of their goods or services, similarly to the prohibition of misleading statements about food safety [14]. Retailers are also required to share liability and not to sell IoT goods with documented security and security defects [19].

*2) Guiding principles:* Encourage the use, globally, of often checked and widely recognized security best practices and guiding principles for design, implementation and use of IoT devices and services [11].

*3) Regulating industrial sectors:* All industries should be subject to fundamental standards such as data security. IoT systems have however been developed and used in different industries and applications, which can lead to stronger protection outcomes through a sectors-based regulatory approach, complementary to core principles [9]. Strong market incentives or current regulation in some industries could reduce the need for new regulation compared to other industries. In the consumer equipment industry, for example, regulatory tools appropriate to the health sector may not be so useful when qualities such as failure tolerance might not be so critical to producing a healthy product [10].

## VI. Conclusion

In this study, authors contributed a method to detect user interface and network service attacks in IoT network. They applied a machine learning approach for classifying the attacks in IoT and WSN. A testbed that contains a number of IoT devices were developed to test the efficiency of the proposed method. A recent dataset IoTID20 which contains 64.2 million of attacks and a total of 63000 attack anomalies were created to measure the performance of IoT attack detectors. Recent approaches in IoT attack detection were compared with the proposed study. Device configuration parameters are the key items to identify an attack in network layers. Usually, attackers modify the configuration in order to launch an attack in IoT environment. In addition, certain policies need to be framed to govern the IoT and WSN. Thus, the proposed study discussed some challenges and necessary policies to monitor the IoT

network. The outcome of the experiment shows that the proposed method capable to detect multiple attacks in IoT and WSN. The future direction of this study is to develop a deep learning-based method to monitor and protect IoT devices from various attacks.

## REFERENCES

[1] Verma, A., Ranga, V. Machine Learning Based Intrusion Detection Systems for IoT Applications. Wireless Pers Commun 111, 2287–2310 (2020). https://doi.org/10.1007/s11277-019-06986-8.

[2] 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.

[3] Md Mamunur Rashid, Joarder Kamruzzaman,Mohammad Mehedi Hassan,Tasadduq Imam, Steven Gordon, " Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques", International journal of environmental research and public health, Vol.17, Issue 9347, 2020 Pp. 1 - 21.

[4] Yu Liu, Zhibo Pang, Magnus Karlsson, Shaofang Gong,"Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control", Building and Environment, Vol. 183, October 2020.

[5] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," in IEEE Access, vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013.

[6] Valentina Timčenko and Slavko Gajin, " Machine Learning based Network Anomaly Detection for IoT environments ",ICIST 2018.

[7] Vibekananda Dutta, Michał Chora´s, Marek Pawlicki ,and Rafał Kozik, "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection",Sensors 2020, Vol. 20,Iss. 4583.

[8] Krawczyk, B., Minku, L. L., Gama, J., Stefanowski, J., & Woźniak, M. (2017). Ensemble learning for data stream analysis: A survey. Information Fusion, 37, 132–156.

[9] Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. https://doi.org/10.1007/978-3-030-47358-7_52 , Accessed: 2020 – 06 – 21.

[10] P. Ducange, G. Mannara, F. Marcelloni, R. Pecori and M. Vecchio, "A novel approach for Internet traffic classification based on multi-objective evolutionary fuzzy classifiers", 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6, July 2017.

[11] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques", IEEE Communications Surveys Tutorials, vol. 21, no. 3, pp. 2671-2701, 2019.

[12] M. F. Elrawy, A. I. Awad and H. F.A. Hamed, "Intrusion Detection Systems for IoT-based Smart Environments: A Survey", J. Cloud Comput., vol. 7, no. 1, pp. 123:1-123:20, December 2018.

[13] V. L. L. Thing, "IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach", 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, March 2017.

[14] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Access, vol. 7, pp. 41525-41550, 2019.

[15] Soe, Yan N.; Feng, Yaokai; Santosa, Paulus I.; Hartanto, Rudy; Sakurai, Kouichi. 2020. "Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture" Sensors 20, no. 16: 4372. https://doi.org/10.3390/s20164372.

[16] S. Ioffe and C. Szegedy, "Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift", Proc. 32nd Int. Conf.on Machine Learning - Vol. 37 ICML'15, pp. 448-456, 2015.

[17] A. L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2):1153–1176, 2016.

[18] T. Hurley, J. E. Perdomo, and A. Perez-Pons. HMMbased intrusion detection system for software defined networking. In Machine Learning and Applications (ICMLA), 2016 15th IEEE International Conference on, pages 617–621. IEEE, 2016.

[19] U. S. R. K. Dhamodharan and R. Vayanaperumal. Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. The Scientific World Journal, 2015:7, 2015.

[20] A. A. Diro and N. Chilamkurti. Distributed attack detection scheme using deep learning approach for internet of things. Future Generation Computer Systems, 2017.

[21] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2):34–42, 2017.