Cyber Security Vulnerability Assessment for IoT-Based Smart Homes

Simranjeet Singh Kapoor
Master of Science in Computer Science
Lakehead University
Thunder Bay, Ontario
singhs@lakeheadu.ca

Manoj Kumar Bhuma
Master of Science in Computer Science
Lakehead University
Thunder Bay, Ontario
mbhuma@lakeheadu.ca

Dr. Dariush Ebrahimi
Department of Computer Science
Lakehead University
Thunder Bay, Ontario
ebrahim@lakeheadu.ca

***Abstract*—With its immense potential, IoT has changed many lives and imprinted them with much more efficiency and accuracy than the conventional approach. A Smart Home is one such impression which IoT has furnished. It has lots of IoT devices connected altogether via the Internet, controlling at fingertips. But with the rapid installation of such devices without proper security conformation, human lives are impacted proportional to the increasing number of various use cases. One of them is Malware attacks. These attacks proved our motivation for this paper. This paper is aimed to secure the devices by bestowing multiple deep learning approaches and compare them to propose the suitable algorithms which prove to be most efficient in classifying the Malware attack on the IoT devices. The Three major approaches compared in this paper for classification are namely the multi-layer perceptron (MLP) which is a type of ANN (Artificial Neural Network), CNN (Convolutional Neural Network), and a Long Short-Term Memory (LSTM) networks which is a type of RNN (Recurrent Neural Network).**

***Index Terms*—Internet Of Things (IOT), SmartHome IoT devices, Long Short-Term Memory (LSTM), Multilayer Perceptron Neural Network (MLPNN), CNN (Convolutional Neural Network),Distributed Denial Of Service (DDoS), Intrusion Detection System (IDS), SMOTE (Synthetic Minority over-sampling technique), RELU (Rectified Linear Unit)**

I. Introduction

The Internet of Things (IoT) is an emerging technology that has grabbed the attention of researchers from every academia and industry. Massive applications of these IoT devices include life-critical applications such as healthcare and the military. Moreover, numerous financial transactions are executed over the Internet every day. This rapid growth of the Internet has led to a significant increase in wireless network traffic too. Some leading studies done by Global - 2020 Forecast Highlights that the wireless network traffic is estimated to account for 2/3 of the overall internet traffic by 2021, with Wi-Fi and cellular devices, predicted to produce almost 66 percent of IP traffic [21]. The idea behind the Internet of things is many information-sensing devices to the Internet to collect all kinds of information needed in real-time. IoT is magnificent in many ways. But unfortunately, this particular technology has not matured yet, and it is not entirely safe. From manufacturers to users, the whole IoT environment still has many security challenges of IoT to overcome. IoT security is considered the subject of demand after several incidents occurred where a specific IoT device was used to infiltrate and attack the more extensive network. Our main emphasis in this paper is on the smart home domain because these industries will incur the worst repercussions in case of security breaches, costing human lives. Thus avoiding such blunder, Smart home IoT devices need more research.

Smarthome is a technology, to be precise, a home, which utilizes internet-connected devices to empower the management and remote monitoring of different devices present in a particular home itself. Here, all the systems and devices operate together, sharing consumer data and performing actions automatically according to consumer preferences. Since all the devices are sender and receivers, they talk with the central unit through messages.

However, these messages are not secured at a time when an attacker attacks the smart home network. Message Authentication is considered one of the major problems in IoT networks. Since with most smart homes system, if an attacker can hold the related network packages, it could lead to various types of attacks such as man-in-the-middle, message modification, denial-of-service could be launched into a smart home. The Internet of things industry must build user trust in the industry to get or be generally embraced. To do so, IoT must ensure its users' protection and privacy. Though it is an active topic of research, there is very little work published, which reviews IoT's security, especially when it comes to the authenticity of messages or Intrusion. This paper analysis conducted into the proposed dataset aimed at the pattern of the IoT system attack in a smart home, and the type of attack was observed as shown in Figure 1. The first way to make the workflow is to analyze and track the information found in the IoT-23 dataset [12]. Benign data was also collected from devices like Somfy door lock, Amazon Echo, Philips Hue. These three devices are used to capture the benign network traffic data in 3 datasets. The Malware capture is distributed in 20 separate folders.

With such growth in usage of IoT devices, Cyber-attacks have witnessed immense growth in rate as the Internet of Things (IoT) is widely used these days. These range from

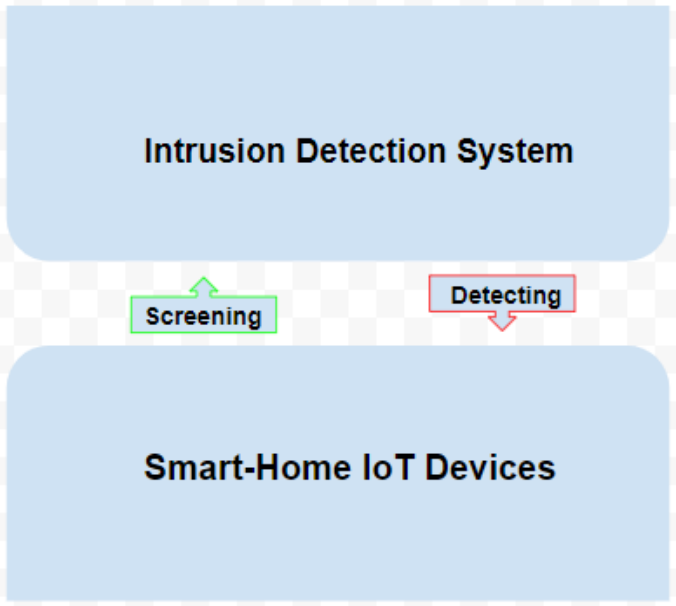

Fig. 1. Overview of an IDS

consumer-oriented devices such as wearables and smart home solutions (Consumer IoT) to connected equipment in the enterprise (Enterprise IoT) and industrial assets such as machines, robots, or even workers in smart factories and industrial facilities (Industrial IoT, the essential component of Industry 4.0). All of these devices are vulnerable and susceptible to network intrusion and should be curbed before a massive attack. Hence this motivates us to code an Intrusion Detection System, thus in this paper, we are proposing and comparing three vital deep learning algorithms namely, ANN (Artificial Neural Network): We'll be implementing a multilayer perceptron (MLP) classifier to detect the anomaly, it is a class of feed-forward ANN. CNN (Convolutional Neural Network): We'll be implementing a CNN, which can train multilayer networks with gradient descent to learn complex, high-dimensional, nonlinear mappings from large collections of data. RNN (Recurrent Neural Network): We'll be implementing an RNN as a discriminative model when the output of RNN is used as label sequences for the input. Long Short-Term Memory (LSTM) networks are a modified version of recurrent neural networks, which makes it easier to remember past data in memory. The vanishing gradient problem of RNN is resolved here [10].

In the following sections, this paper will discuss Literature Review, Methodology, Performance Evaluation, Results, Conclusion and Future Work.

II. Literature Review

Smart wireless sensors in smart home applications have become one of the most engaging devices for monitoring and home automation; they have also become the target of numerous attacks. Numerous intrusions related to the availability of (1)services availability, (2) network routing, and node authentication are observed. These smart homes are vulnerable to numerous attacks, although many advantages are obtained from IoT-based smart homes. Using its network or local communication interface, an entity can directly target an interconnection system or field system, and a device can be impersonated using its fake certificate. Used this home gateway, household appliances can be connected to a wired or wireless network. Household devices can connect to a wired or wireless network through this home gateway. An attack on the home portal would lead directly to an attack on the entire household network, as there is a potentially vulnerable external connection [1]. The study by Tong et al. proposed a safety model for protecting the flow of knowledge in a smart grid's home area network [2]. Using confidential and non-confidential information flow rules, the proposed model will efficiently control the information flow in a home area network without compromising the usual functionality of the home area network. The study by Yang et al. suggested a phone-out-only policy and a virtual environment strategy in order to achieve improved protection and security for remotely managed, and controlled systems [3]. The purpose of the phone-out-only policy was to ensure that only the smart home devices from the indoor side initiate contact between the smart home devices and the remote users.

The first integrated training and testing datasets are developed through an efficient allocation-based least square SVM (OA-LS-SVM) by Kabir et al. [4]. Then the amount of training and testing sets is calculated by an optimal allocation (OA) method. Consequently, sample sizes have been chosen directly from training and testing datasets for the classifier. Although the authors in this paper provided some interestingly satisfactory outcomes, due to its restriction of the training dataset to samples having a particular relationship with the present instance, some essential details or features in the dataset might be missing. Also, extracting all the pieces from training and research datasets is a challenging task to resolve. The authors focus on designing a lightweight IDS for IoT detection of anomalies. To detect an adversary attempting to insert unwanted data into the IoT network, they developed a lightweight attack detection technique using a supervised machine learning-based support vector machine (SVM) [5]. The target is a standard method of attack, known as DDoS. Two fundamental problems are centred on the suggested IDS: the receiving data used to classify the signal and the classifier based on machine learning. Their work mainly focused on DDoS attacks, whereas we consider multiple attacks, including DDoS in our dataset.

Many IoT scenario analysis is only directed at their data sets from IoT networks. As several vendors use different network protocols, the network complexity increases with IoT networks, making it challenging to implement encryption and authentication schemes. Besides, the lack of publicly accessible IoT-specific datasets makes it increasingly difficult

for researchers to perform experiments. The NSL-KDD dataset and DARPA dataset are the most used datasets by researchers to design new IDS [6]. The issue with these two datasets is that neither of the two datasets was built to resemble a loT network. And concern with these experimental datasets is that both datasets were generated more than a decade ago, meaning that neither the network activities of existing networks nor recent cyberattacks such as the botnet attacks cannot be represented. The latest edition of 2020 is updated with cyber threat kits.

III. Methodology

An Intrusion Detection System is a monitoring system that looks for unusual activity and generates warnings when it does. Different types of machine-learning and Deep learning models have been leveraged in anomaly-based Intrusion Detection System. This paper aims to propose an IDS by using deep learning algorithms novice enough to detect the anomaly in all variants of cause. This paper proposed Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) in RNN, Multilayer Perceptron Neural Network (MLPNN) to compare and offer the robust DL model for IDS.

A. Type of Attacks

Our model basically addresses seven types of attacks

1) *Part Of A Horizontal Port Scan*: Horizontal scanning is described as attempting to search a group of IP addresses for a single port. A horizontal scan is a port scan that scans several hosts for the same port. Most of the time, the attacker is aware of a specific weakness and is looking for devices that are vulnerable [16].

2) *C&C-File Download*: Some of the computers in a botnet are under the control of C&C servers. It can distribute commands that are used to steal data, disrupting operation, spreading malware, and more. Under the C & C-File Download infection, the server has taken control of the system and is sending a file to the victim's computer [12].

3) *Okiru*: In the same way that Mirai searches for systems with default Telnet passwords, the Okiru malware has similar functionality with high-level architecture. To gain control of victim networks, Okiru utilizes its collection of configurations and botnet command-and-control servers, as well as several exploits [17].

4) *Distributed Denial Of Service (DDoS)*: A Distributed Denial of Service (DDoS) attack involves flooding a server with malicious traffic to make it inaccessible [18]. Because of the large number of flows directed to the same IP address, these traffic flows are identified as part of a DDoS attack. There are different types of DDoS attacks which can be distinguished as shown in Figure 2.

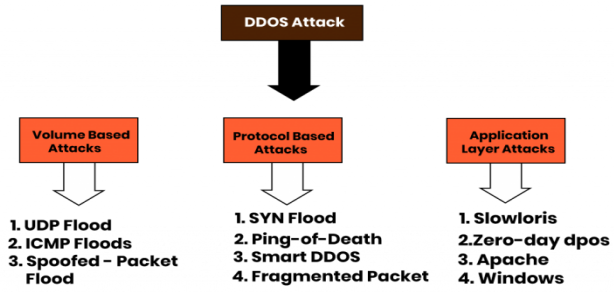

Fig. 2. Types Of DDoS Attacks [19]

5) *Command & Control*: Here infected network was linked to a CC server, as indicated by C&C. Since the connections to the suspicious server are periodic, or our infected network is downloading binaries from it, or any decoded instructions are coming and going from it, this behaviour was found in the network malware capture study [12].

6) *File Download*: A file is being downloaded to our infected computer, according to this target. This is detected by combining any known suspicious destination port or destination IP known to be a C&C server with connections with response bytes more significant than 3KB or 5KB [12].

7) *C& C-Torii*: Unlike other IoT botnets, this one tends to be more stealthy and persistent once the system has been breached, and it doesn't function like other botnets like DDOS, which targets all connected devices, or, of course, cryptocurrency mining. Instead, it includes a robust collection of features for sensitive data, as well as a modular architecture capable of fetching and executing other commands and executable code, all of which is accomplished through multiple layers of encrypted communication. [20].

B. Dataset

The dataset considered in this paper is named "IoT-23", a new dataset of network traffic from IoT devices [12]. It was first published in January 2020, with captures ranging from 2018 to 2019. It was captured in the Stratosphere Laboratory, AIC group, FEL, CTU University, Czech Republic. This dataset and its research are funded by Avast Software, Prague. Its goal is to offer a large dataset of real and labeled IoT malware infections and IoT benign traffic for researchers to develop machine learning algorithms. It has 20 malware captures executed in IoT devices, and 3 for benign IoT devices traffic. The network traffic captured for the benign scenarios was obtained by capturing the network traffic of three different

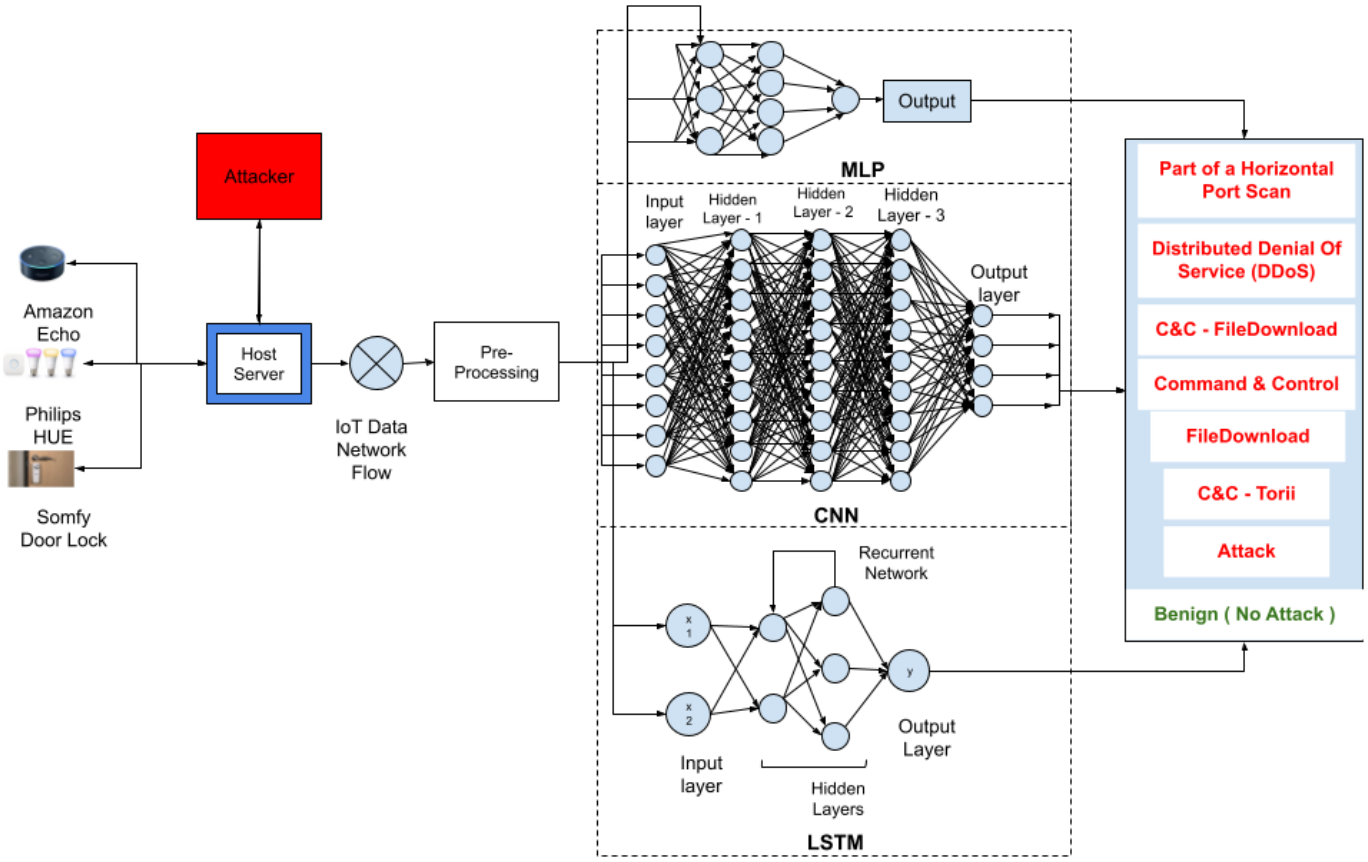

Fig. 3. System Architecture for MLP, CNN and LSTM

IoT devices: (1) Philips HUE smart LED lamp (2) Amazon Echo home intelligent personal assistant and (3) Somfy smart door lock. For the rest of the 20 malware captures. The three most common malicious (not benign flows) labels are: (1) "Part Of A Horizontal Port Scan" (213,852,924 flows) , (2) "Okiru" (47,381,241 flows) and (3) "DDoS" (19,538,713 flows). While the three least common malicious (not benign flows) labels are: (1) C & C-Mirai (2 flows), (2) C & C-HeartBeat-FileDownload (11 flows). A port scan is an attack that sends client requests to a range of server port addresses on a host, intending to find an active port and exploit a known vulnerability of that service [24].

C. Proposed Structure

Our analysis of this data set was to observe the pattern and predict the form of attack one can make on IoT devices in a Smart Home. The first method of allowing the workflow is by evaluating the data in it and testing the information for which we utilized the IoT-23 dataset. Data from various devices such as Somfy Door Lock, Amazon Echo, Philips Hue were acquired and assigned as benign. The major source of malware was captured from 20 main zipped files of IoT-23. The proposed deep learning techniques made sure that the we have maximum dataset within our model without compromising the machine's computing limitations. Most of the cited research papers are primarily focused upon DDoS attacks. They have tried to develop an Intrusion Detection System(IDS) using Machine Learning approaches such as KNN, Random Forest, and so on. From our study, we found that conventional ML schemes rely primarily on feature engineering, measuring the correlation between features is often time-consuming and complicated. Therefore, detecting attacks by introducing conventional ML algorithms in real-time implementations is impractical. To overcome this pitfall, We are trying to implement deep learning approaches that cover MLPNN, LSTM, and CNN. Since there is not more research work done on these Deep Learning methods especially combining Smart Home Networks as shown in Figure 3, which depicts the System Architecture that consists of Deep Learning Algorithms used to detect different intrusions (shown in architecture).

D. Data Preprocessing

This is the first step towards the implementation where the dataset is preprocessed in a way that the transformed data gets more consistent and valuable. To achieve that understandable data, more useful features are extracted from the set of all

features in dataset.

1) Feature Extraction: Feature extraction is the first step after data collection [13]. Here, the dataset is refined by removing hidden values, null values and also can extract features which include IP addresses, port numbers, network protocol, transmission flow, and the network connection frequency, which is associated with their respective attacks. Feature extraction is one of the most important processes in cleansing the dataset hence we consider using the two most powerful filter-based algorithms.

1) *Pearson's correlation*:
It shows the correlation with The target column to the training columns (i.e. X) and shall be considered before it is trained for the final model, considering it as predictor variables. A heat map is plotted to validate the association with associated columns. In order to validate the correlation with the target column, 'detailed label, the correlation coefficient of Pearson is measured in a numerical column as shown in Figure-6. In this Heat Graph, more the intensity of red, more the dependency of one variable on the other, whereas the blue intensity represents the less dependability of that particular column. The X-axis and Y-axis both represents columns dataset has.

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum)^2][n\sum y^2 - (\sum y)^2]}}$$

Where,
r = Pearson Coefficient of Correlation,
n = number of rows,
x = first column/variable,
y = secound column/variable,

For instance, in Figure-5 , if the last row is checked, bottom column "detailed-label" which is totally dependent upon "proto_tcp" as the value is approaching towards 0.92 which is red in intensity. Similarly, the nearby column has value "-0.9" which represents that the same "detailed-label" column is not related to "proto_udp " column. The Formula behind calculating these values is correlation factor or also known coefficient.

2) *Chi-square test*:
Chi-squared test is performed to testify whether the two categorical variables are highly related. This statistical concept is mostly used for selecting important features and attributes since a wide amount of irrelevant features can significantly increase the time complexity of training the training time of the model and thus increase the probability of data overlaps. It is plotted as shown in Figure 4.

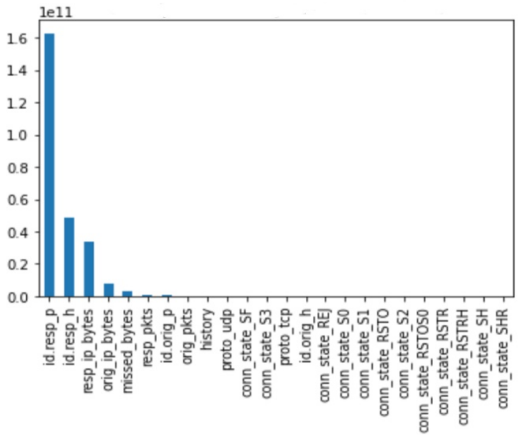

Fig. 4. Chi-Squared Correlation Plot

2) Train-test Split: After feature selection, the dataset is converted into (.csv) format and is split into train and test datasets for classifications. The classes are too unbalanced to train all three DL models. So it is required to Balance each class and make all classes in equal proportion. The majority of classes are being under-sampled here. It picks randomly some of the data points in a selected number.
Part of a horizontal port scan and Benign classes are being under-sampled to 100,000 data points each. Synthetic Minority over-sampling technique (SMOTE) is used to achieve the same. It is a technique that adds the synthetic data to the minority samples present in the data which mimics the original data. So, it is one of the proven techniques in oversampling minority classes and treating class imbalance. The other classes of attacks like C&C, DDoS, Attack, C&C Torii, C&C- File Download, File Download are being over sampled to 100,000 data points each. The data is being split into training and testing data sets with an 80:20 ratio after class balance.

IV. Performance Evaluation

The performance evaluation of any IDS performance can be done by adopting the fundamental model of performance measures namely accuracy, DR, false alarm rate (FAR), Precision, F1 score, CPU Time to Build Model (TBM), and CPU Time to Test (TT). Accuracy shows the overall effectiveness of an algorithm whereas DR, also known as Recall, refers to the number of posed attacks detected divided by the total number of posed attack instances in the test dataset. One can also extend this to confusion matrix plot for multi-class classification predictions.

A. Performance Metrics

Our proposed model is evaluated with the help of various performance metrics such as Accuracy, Precision, Recall and F1-score. Basic terminologies which are used to evaluate

Fig. 5. Pearson Correlation Heat-map Graph

these metrics are as follows:

- *True Positive(TP):* When the predicted value is positive (malicious) and the actual value is also positive.
- *True Negative(TN):* When predicted value is negative (benign) and the actual value is also negative.
- *False Positive(FP):* When the model incorrectly predicts positive (malign) value while the actual output is negative (benign).
- *False Negative(FN):* When the model incorrectly predicts negative (benign) value when the actual value is positive (malign).

1) Accuracy: Accuracy is the ratio of correctly classified values over all the predictions made by the model. It can be computed as shown in the equation 1.

$$Accuracy = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{1}$$

2) Precision: Precision is the ratio of number of correct classifications to the number of total positive results, including those incorrectly identified as positive. It can be computed as shown in equation 2.

$$Precision = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{2}$$

3) Recall / Sensitivity: Recall is the ratio of number of correctly predicted positive values to the number of total number of records, including both incorrectly identified as negative (that should have been identified as positive) and the ones identified positive. It can be computed as shown in the

given equation 3.

$$Recall = \frac{\text{TP}}{\text{TP + FN}} \tag{3}$$

4) F1-Score: F1-Score is the harmonic mean of Precision and Recall. Equation 4 computes F1-Score.

$$F1 - Score = \frac{\text{2 x Precision x Recall}}{\text{Precision + Recall}} \tag{4}$$

B. Model Evaluation

A total of three deep learning models are classified in order to identify malicious packets in the Smart Home environment. This section involves the performance of every model along with the efforts done to increase the accuracy of these models.

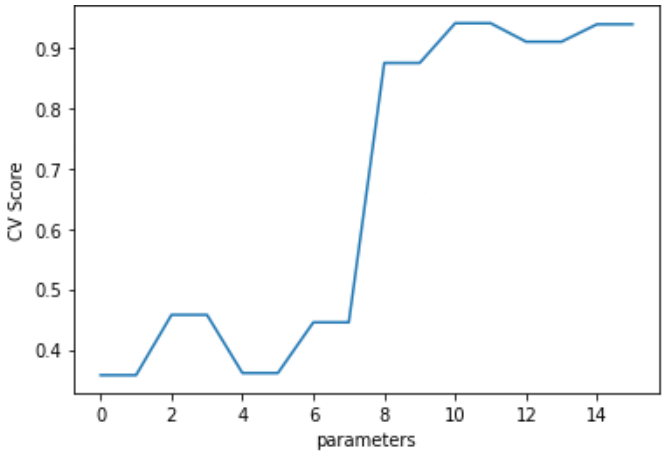

Fig. 6. Validation Accuracy in MLP-NN

1) MLP-NN: The Multi-Layer Perceptron Neural Network has been trained on the specified dataset. The results of the trained Neural Network were quite realistic, classifying 8 types of attacks stated in the dataset. While training the tuned model with the best parameters found via the Grid-Search-CV method, it is plotted with the parameters and how with every tuned model the Cross Validation (CV) score is improving leading to greater accuracy of the MLP model. While performing the model, the CV score was fluctuating with increase in Hyperparameters and the best score is taken after 10 parameters, The plotted Figure 6 illustrates that there is no significant increase in CV score after 8 parameters were reached .

2) CNN: The CNN model implied in this paper is made up of two layers CONV-1D i.e. convolution 1-D. Each layer is having a pooling (down-sampling) layer followed by the batch normalization and a specified percentage dropout of neurons. The first layer is with 16 filters of size 2, max-pooling of filter size 1, batch normalization & 20% dropouts of connections. The second layer is with 32 filters of size 2 i.e., doubled off the previous layer, max-pooling of pooling size 2, batch normalization, and 50% dropouts of connections.

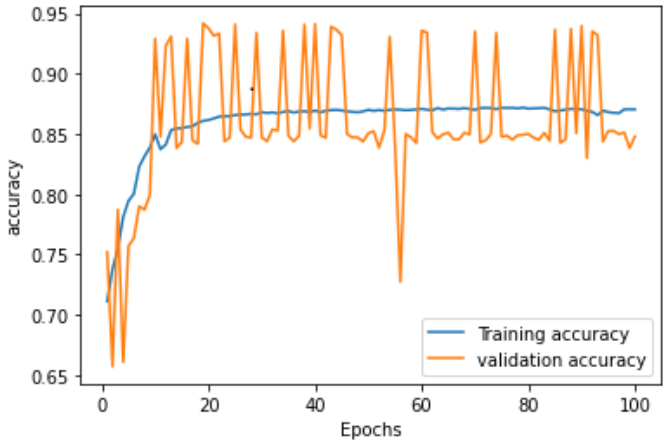

Fig. 7. Training & Validation accuracy for CNN

As the plotted Graph 7 evident that the CNN model has resulted after training by projecting 94.43% validation accuracy on test data with 94.81% accuracy on training data. The loss & accuracy while training as shown is approaching slightly more towards zero and 90% respectively, validation in 50 epochs. The accuracy plot shows the model is optimized quite well at an accuracy of around 95% accuracy. It is observed a small difference while training and validating the model which shows how accurately the CNN model is performing on any unknown data post-training. Since the accuracy is changing after every epoch, its found that the model was performing more or less the same in 60-80 range of epochs. The accuracy value is the same after 70 epochs. Hence we stopped at 100 epochs.

CNN which is identified as a feed-forward Neural Network. Each layer in this CNN architecture certainly has its own functionality that defines the hidden layers and implements extraction of features [14]. CNN also has the benefit of feature selection and extraction without human interference. To train the classifier who could detect intrusion, the collected data and generated data will be used.The last hidden layer is a fully connected layer that is flattened i.e, converts multidimensional output array to one single dimensional array to pass through the final dense layer. The dense layer in our CNN model with 64 units output space and dropout of 50% connections.

All these three layers are activated with a “ReLU (Rectified

Linear Unit)" activation function except the last classifying layer which has a Sigmoid classification layer with a dense output of 8 units since the dataset has 8 output labels for classification.

3) LSTM: The plots shown by the LSTM model as shown in Figure 8 have the improvement of network modeling consequently by each epoch. It has experimented with different batch sizes, epochs, layers. The results produced are found to be optimized for around 90.78% validation accuracy in a total of 400 epochs . Here accuracy has keep on increasing with the number of epochs and there is not much problem of over-fitting of the network.

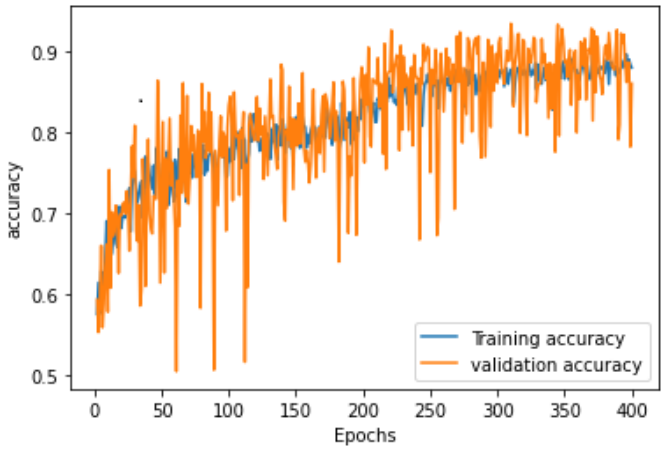

Fig. 8. Training & Validation accuracy for LSTM

The fluctuations while training the model were observed. LSTM layer is comprised with two-layers, Layer-1 is the sequential model is designed with an LSTM layer of 100 LSTM units present in it. This layer is activated with RELU as an activation function for all cells present in it. Whereas the Layer-2 is used as a dense layer that outputs the required number of classes. IoT-23 dataset has 8 different classes as its target. So, the dense layer outputs probabilities corresponding to 8 classes. This layer has been activated using a softmax function because it is generally preferred to have a softmax function for Multi-Class Classification. This network is compiled with Adam optimizer and accuracy as metrics for evaluation. In each epoch, the results are improved based on categorical cross-entropy as loss function.

Then, the model is trained on IoT-23 dataset in batches of 10,000 rows through the above LSTM network. While training the above network it also validates the results on a test dataset that is 20% of the remaining dataset available.

C. Results and Experiment Analysis

For classification, the aim is to identify the best-performed algorithm from CNN, LSTM, MLPNN. LSTM is capable of processing single data as well as full data sequences.

CNN is a sequential combination of convolution and pooling layers that can be used to identify the important features from the dataset. To gain the final output, these layers are linked with a few fully connected layers [15]. However, the aim of using multiple convolution and pooling layers is to discover different scales of complex hierarchical features from the given data.

MLP-NN has resulted in a training accuracy of 95% while the validation accuracy results as 94%. Also while evaluating the model on 20% set-aside test data it has given the same accuracy of 95% on it. So, the MLP model is said to be 95% accurate in classifying the 8 types of attacks in a smart home domain. Whilst verifying other metrics from the classification report precision, recall, f1 score macro averages are given as 95% each. Finally, the designed MLP neural network can detect the pattern in attacks that are observed in smart homes using IoT and concretely commit 95 out of 100 predictions correctly. This classification report and confusion matrix is shown in Table I:

	Precision %	**Recall%**	**F1 Score%**	**Support%**
Attack	0.99	1.00	0.99	20000
Benign	0.97	0.84	0.90	20000
C&C	0.85	1.00	0.92	20000
C&C-File Download	1.00	1.00	1.00	20000
C&C-Torii	0.97	1.00	0.98	20000
DDoS	0.99	0.99	0.99	20000
File Download	1.00	1.00	1.00	20000
Horizontal Port Scan	0.85	0.77	0.81	160000
Accuracy			0.95	160000
macro avg	0.95	0.95	0.95	160000
weighted avg	0.95	0.95	0.95	160000

TABLE I
CLASSIFICATION REPORT FOR MLP-NN

The CNN model has a training accuracy of 87% while the validation accuracy of the same model is 94% as referred from Figure 7. The other results that are evaluated the network of test data of 20% available are precision, recall and f1-score where the macro averages are given as 96%, 94%, 94% respectively. The classification report can be conformed through the stated results as shown in Table II.

LSTM network has given very promising results with validation accuracy of 93.34% with a training accuracy of 86% which can be refereed from Figure 8. The difference between training and validation accuracy scores is in 5% range. This shows that the LSTM recurrent neural network can produce the same results on unknown data. The other results that are checked while evaluating the network on test data of 20% available are precision, recall, f1 score which are produced as 94%, 93%, 93% respectively of macro averages and weighted averages. This shows the network can produce more than 90% accurate results on the IoT-23 smart home data available. The classification report is shown in Table III.

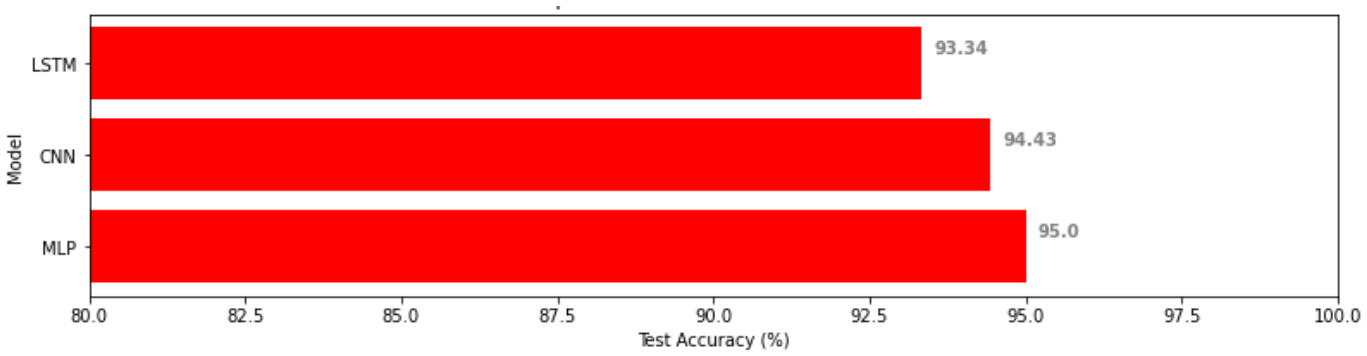

Fig. 9. Comparing DL Models

	Precision%	Recall%	F1 Score%	Support%
Attack	1.00	1.00	1.00	20000
Benign	0.99	0.97	0.98	20000
C&C	0.71	1.00	0.83	20000
C&C-File Downld	1.00	1.00	1.00	20000
C&C-Torii	0.98	1.00	0.99	20000
DDoS	1.00	0.99	1.00	20000
File Download	1.00	1.00	1.00	20000
Horiz-Port Scan	0.98	0.60	0.74	160000
Accuracy			0.94	160000
macro avg	0.96	0.94	0.94	160000
weighted avg	0.96	0.94	0.94	160000

TABLE II
CLASSIFICATION REPORT FOR CNN

	Precision	Recall	F1 Score	Support
Attack	1.00	0.99	0.99	20000
Benign	0.97	0.87	0.92	20000
C&C	0.76	1.00	0.86	20000
C&C-File Download	1.00	1.00	1.00	20000
C&C-Torii	0.92	1.00	0.96	20000
DDoS	1.00	0.99	0.99	20000
File Download	1.00	1.00	1.00	20000
Horizontal Port Scan	0.87	0.62	0.72	160000
Accuracy			0.93	160000
macro avg	0.94	0.93	0.93	160000
weighted avg	0.94	0.93	0.93	160000

TABLE III
CLASSIFICATION REPORT FOR LSTM

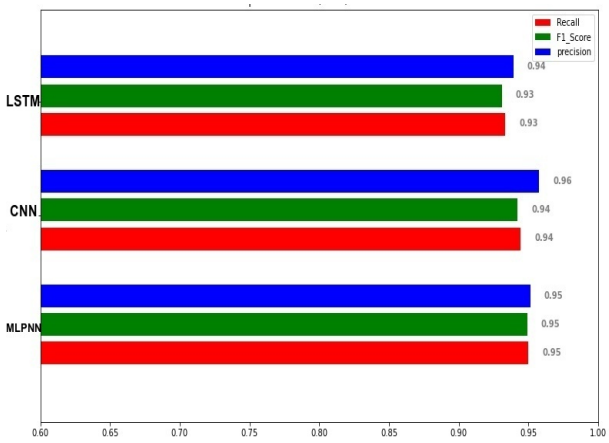

Fig. 10. Performances Of DL Models

D. Comparison of Models

As stated above the IoT-23 dataset is implemented with three different models like MLP, CNN. LSTM. The results are compared as displayed in Figure 10 after the dataset is cleaned, prepossessed, visualized, and extracted useful features from the large dataset available. The results shows that the most efficient algorithm among these three is MLP-NN Model which has an accuracy of 95% resulting in 1% more accurate than CNN and 2% accurate than LSTM. Other performance metrics such as Recall, F1-Score and Precision were are also compared as illustrated in Figure 10.

Nicolas-Alin Stoian et al. proposed a paper working on IoT-23 dataset [22]. This paper proposes a Machine Learning method on the IoT-23 dataset, the authors claimed the best algorithm for anomaly detection is random forest. It is harder to depict why random forest was most suitable, it is also suggested that there is a need for research in since IoT-23 dataset is quite novice to work. According to the authors, random forest works best when metric scores are high when they compare the findings to other related dataset Also, more complex algorithms such as neural networks have been tested, simpler algorithms always had a certain edge over the more complex ones.

Vibekananda Dutta et al. proposed a paper on 3 different datasets [23]. This paper proposes a deep learning approach on the IoT-23, LITNET-2020, NETML-2020. Authors reported in the paper as this study dealt with a group approach that incorporated deep learning algorithms using a stacked generalisation concept for an effective network intrusion detection system based on anomalies. To achieve the highest efficiency, various feature engineering methods were combined with dimensionality reduction in this paper. A combination of DNN and LSTM followed by a meta-classifier resulted in a significant performance of the latest network traffic data sets and detection of anomalies. The efficiency of the

proposed stacked ensemble framework was assessed by three heterogeneous datasets, IoT-23, LITNET-2020 and NetML-2020 as illustrated in Table IV.

Study	Method	Dataset	Accuracy/Precision
Dutta et al. [23]	Random Forest	IoT-23	0.893
Dutta et al. [23]	DNN	IoT-23	0.984
Dutta et al. [23]	LSTM	IoT-23	0.991
Dutta et al. [23]	Stacked	IoT-23	0.997
Stoian et al. [22]	Naive Bayes	IoT-23	0.76
Stoian et al. [22]	ANN	IoT-23	0.71
Stoian et al. [22]	SVM	IoT-23	0.6
Stoian et al. [22]	AdaBoost	IoT-23	0.86
Stoian et al. [22]	Random Forest	IoT-23	0.995
Our Proposed	MLP	IoT-23	0.95
Our Proposed	CNN	IoT-23	0.9443
Our Proposed	LSTM	IoT-23	0.9334

TABLE IV
RESULT COMPARISON

V. FUTURE WORK & CONCLUSION

For this domain of research, most Intrusion Detection Systems utilize deep learning and data science is used as a preprocessing technique. Using deep learning for IDS is particularly for bi-clustering is very useful. This research is an investigation of deep learning approaches to get a deeper understanding of how the way of using it can be applied in IDS. Finally, we discuss what will come next in the implementation of IDS in the future.

Three neural networks have been employed, MLP, CNN, and LSTM to complete the work This suggests that at least 90% of the attacks in the Internet of Things can be detected and categorized as belonging to one of the three types. a large dataset has been gathered for training and testing the three neural networks This dataset would make it possible for the models to obtain much more insight from the same features in the future Accuracy is going to be much better in predicting and classifying threats. It has been stated that the models are resilient to any kind of data going to come from smart home IoT environments, and can identify breaches. The study can be generalized to incorporate other neural networks in the future.

REFERENCES

[1] Ricquebourg, V.; Menga, D.; Durand, D.; Marhic, B.; Delahoche, L.; Loge, C. The Smart Home Concept: Our Immediate Future. In Proceedings of the 2006 1st IEEE International Conference on E-Learning in Industrial Electronics, Hammamet, Tunisia, 18–20 December 2006; pp. 23–28.

[2] Tong, J.; Sun, W.; Wang, L. An Information Flow Security Model for Home Area Network of Smart Grid. In Proceedings of the 2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Nanjing, China, 26–29 May 2013; pp. 456–461.

[3] Yang, L.; Yang, S.H.; Yao, F. Safety and Security of Remote Monitoring and Control of Intelligent Home Environments. In Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 8–11 October 2006; Volume 2, pp. 1149–1153.

[4] E. Kabir, J. Hu, H. Wang, and G. Zhuo, "A novel statistical technique for intrusion detection systems," Future Gener. Comput. Syst., vol. 79, pp. 303–318, Feb. 2018.

[5] Sana Ullah Jan, Saeed Ahmed, Vladmit Shakhov, and Insookoo , "Toward a Lightweight Intrusion Detection System for the Internet of Things," March 28. 2019.

[6] Bakhtiar, F. A., Pramukantoro, E. S., Nihri, H. (2019, March). A Lightweight IDS Based on J48 Algorithm for Detecting DoS Attacks on loT Middleware. In 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech) (pp. 41-42). IEEE.

[7] Benkhelifa, E., Welsh, T., Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for loT: Toward universal and resilient systems. IEEE Communications Surveys & Tutorials, 20(4), 3496-3509.

[8] N. Farnaaz and M. A. Jabbar, Random forest modeling for network intrusion detection system,Procedia Comput. Sci., vol. 89, pp. 213.217,May 2016

[9] L. van Efferen and A. M. Ali-Eldin, "A multi-layer perceptron approach for flow-based anomaly detection," in Proc. Int. Symp. Netw., Comput. Commun. ISNCC, May 2017, pp. 1-6.

[10] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, p. 436, 2015.

[11] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018, pp. 29–35.

[12] Stratosphere Laboratory. A labeled dataset with malicious and benign IoT network traffic. January 22th. Agustin Parmisano, Sebastian Garcia, Maria Jose Erquiaga.

[13] Sara Al-Emadi, Aisha Al-Mohannadi, Felwa Al-Senaid (2020). 'Using Deep Learning Techniques for Network Intrusion Detection', 978-1-7281-4821-2/20/ Department of Computer Science and Engineering.

[14] Pham Van Huong, Le Due Thuan, Le Thi Hong Van, Dang Viet Hung, 'Intrusion Detection in IoT Systems Based on Deep Learning Using Convolutional Neural Network', (2019) 6th NAFOSTED Conference on Information and Computer Science (NICS).

[15] Nogovitsyn, N., Souza, R., Muller, M., Srajer, A., Hassel, S., Arnott, S.R., Davis, A.D., Hall, G.B., Harris, J.K., Zamyadi, M. and Metzak, P.D., 2019. Testing a deep convolutional neural network for automated hippocampus segmentation in a longitudinal sample of healthy participants. NeuroImage, 197, pp.589-597.

[16] Bailey Lee, C., Roedel, C., &; Silenok, E. (2003). Detection and Characterization of Port Scan Attacks, University of California, San Diego.

[17] Lewis, N. (2018, August 13). Okiru malware: How does this Mirai malware variant work SearchSecurity. https://searchsecurity.techtarget.com/answer/Okiru-malware-How-does-this-Mirai-malware-variant-work

[18] Vanitha, K., UMA, S. V., &; Mahidhar, S. (2017). Distributed denial of service: Attack techniques and mitigation. 2017 International Conference on Circuits, Controls, and Communications (CCUBE). doi:10.1109/ccube.2017.8394146

[19] V. (2019, December 19). What is a DDoS attack? How to Stop DDoS Attacks? Testbytes. https://www.testbytes.net/blog/ddos-attack/

[20] New Torii Botnet uncovered, more sophisticated than Mirai — Avast. (2018). Torii Botnet - Not Another Mirai Variant. https://blog.avast.com/new-torii-botnet-threat-research

[21] Cisco Annual Internet Report (2018–2023) (March 9, 2020) https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[22] Nicolas-Alin Stoian (2020) University of Twente PO Box 217, 7500 AE Enschede the Netherlands n.stoian@student.utwente.nl

[23] Dutta, Vibekananda & Choraś, Michał & Pawlicki, Marek & Kozik, Rafał. (2020). A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection. Sensors. 20. 4583. 10.3390/s20164583.

[24] Port Scan attacks and its detection methodologies (Theory) : Virtual Intrusion Detection Lab : Computer Science Engineering : Amrita Vishwa Vidyapeetham Virtual Lab. (2011). Vlab Amrita. https://vlab.amrita.edu/?sub=7brch=199sim=362cnt=1