Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes

Simranjeet Singh Kapoor
Master of Science in Computer Science
Lakehead University
Thunder Bay, Ontario
1093604

Manoj Kumar Bhuma
Master of Science in Computer Science
Lakehead University
Thunder Bay, Ontario
1101603

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

***Abstract*—IoT with its immense potential 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. This proved as 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 proves 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*—SmartHome IoT devices, Long Short-Term Memory (LSTM), Multilayer Perceptron Neural Network (MLPNN), CNN (Convolutional Neural Network)**

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 includes life-critical applications such as healthcare, and the military. Moreover, numerous financial transactions 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. The idea behind Internet of things is a large number of 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. The whole IoT environment, from manufacturers to users, still have many security challenges of IoT to overcome. IoT security is considered as the subject on demand after a number of incidents where a common IoT device was used to infiltrate and attack the larger network.Our main emphasis in this paper is on smart home domain because these industry will incur the worst repercussions in case of security breaches, costing human lives as well. Thus avoiding such blunder, Smart home IoT devices needs more research.

Smart home 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 among themselves and performing actions automatically according to consumer's preference. Since all the devices are sender and receivers, they talk with central unit through messages.However, these messages are not secured at a time when attacker attacks the smart home network. Message Authentication is considered as 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 smart home. The Internet of things industry must build user trust in the industry now, to get or be generally embraced. In order to do so, IoT must ensure its users' protection and privacy. Though it is a yet an active topic of research, there is very little work published , which review the security of IoT 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. The first way to make the workflow is to analysis and track the information found in the IoT-23 dataset. The 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 dataset. The Malware capture is distributed in 20 separate folders.

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

Identify applicable funding agency here. If none, delete this.

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]

II. Literature Review

Smart wireless sensors in smart home applications have become very attractive devices for monitoring and tracking moving objects; they have also become the target of numerous attacks. Numerous intrusion 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 potential 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. 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 [2]. 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. 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 [3]. Kabir et al. developed an efficient allocation-based least square SVM (OA-LS-SVM). They first integrated training and testing datasets by this technique. Then the amount of training and testing sets is calculated by an optimal allocation (OA) method. Consequently, sample sizes have been choosen directly from training and testing datasets for the classifier. Although 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 sample, some essential details or features in the dataset might be missing. Also, extracting all the samples from training and research datasets is a challenging task to resolve [4]. The authors focuses on designing a lightweight IDS for IoT detection of anomalies. In order to detect an adversary attempting to insert unwanted data into the IoT network, they designed a lightweight attack detection technique using a supervised machine learning-based support vector machine (SVM). The target is a common method of attack, known as DDoS. Two key problems are centred on the suggested IDS; the attribute of the receiving data used to classify the signal and the classifier based on machine learning. Their work mainly focused on DDoS attack whereas we consider multiple attacks including DDoS in our dataset [5].Many loT scenario analysis is only directed at their data sets from loT networks. Because of such apparent obstacles,they continues to exist with the risk. As several vendors use different network protocols, the network complexity increases with loT networks, making it difficult to implement encryption and authentication schemes. In addition , the lack of publicly accessible loT-specific datasets makes it increasingly difficult for researchers to perform experiments. The NSL-KDD dataset and DARPA dataset are the mostly used datasets by researchers to design new IDS. The issue with these two datasets is that neither of the two datasets were 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. [6].

III. Dataset

The dataset considered in this paper is named as "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 is 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 IoT devices: (1) Philips HUE smart LED lamp (2) Amazon Echo home intelligent personal assistant and (3) Somfy smart door lock.For rest of the 20 malware captures. The three most common malicious (not benign flows) labels are: (1) PartOfAHorizontalPortScan (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) PartOfAHorizontalPortScan-Attack (5 flows) and (3) C & C-HeartBeat-FileDownload (11 flows). A port scan is an attack that sends client requests to

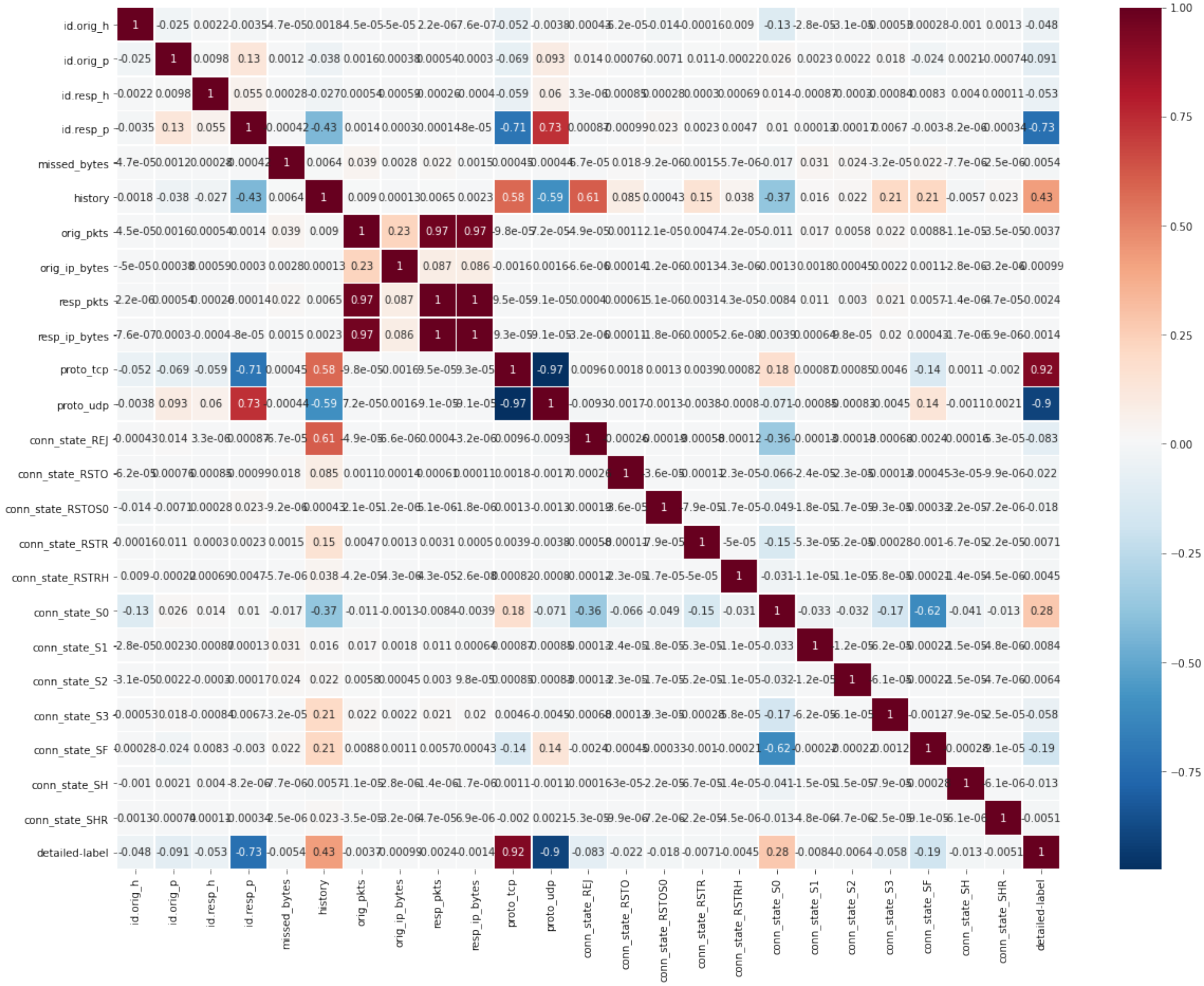

Fig. 1. Pearson Correlation Heatmap Graph

a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.

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 includes IP addresses, port numbers, network protocol, transmission flow and the network connection frequency, which associated with their respective attacks. Feature extraction is one of the most important process in cleansing the dataset hence we consider using two most powerful filter based algorithms namely chi-square and Pearson's correlation. The target column correlation with the training columns (i.e. X) shall be considered before it is trained for final model, considering it as predictor variables. That is why 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 Fig 1. The Formula to calculate the correlation factor or coefficient is shown :

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

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

Another insights gathered for the IoT-23 dataset is Chi-Squared A 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 model and thus increase the probability of data overlaps. It is plotted as show in Fig 2.

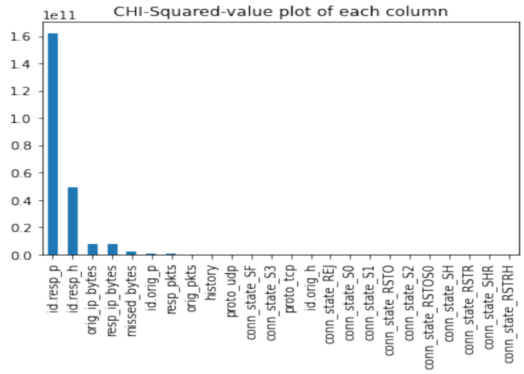

Fig. 2. Chi-Squared Correlation Plot

After feature selection the dataset is converted into (.csv) format and is split into train and test dataset for classifications. For classification we aim to identify the best performed algorithm from CNN, LSTM, MLPNN. LSTM is capable of processing single data as well as full data sequences.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.

IV. Proposed Structure

Our analysis on this data set was to observe the pattern and predict the form of attack one can make on a IoT devices in an 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 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 covers MLPNN, LSTM, and CNN. Since, there are not more research work done on these Deep Learning methods especially combining Smart Home Networks.

Our objective is to build an intrusion detection system by using deep learing algorithms namely the Convolutional Neural Network (CNN) ,Long Short-Term Memory (LSTM) in RNN, Multilayer Perceptron Neural Network (MLPNN). In terms of test and train time, efficiency, and speed, considering the metrics such as accuracy, precision, recall, and f1 score we aim to find the most effective deep learning algorithm for the Intrusion Detection Model in IoT.

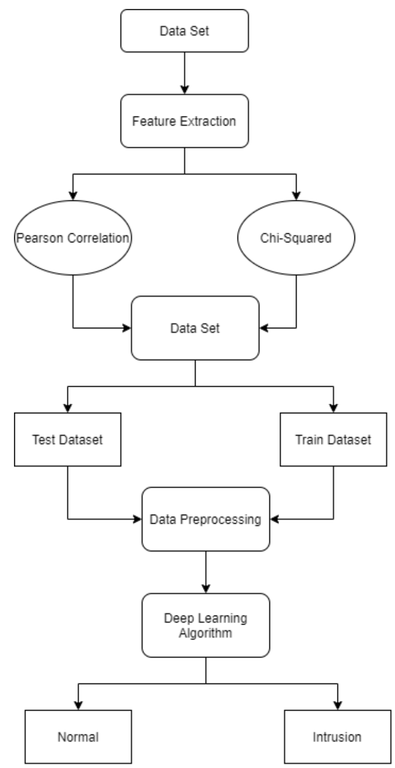

Fig. 3. System Architecture

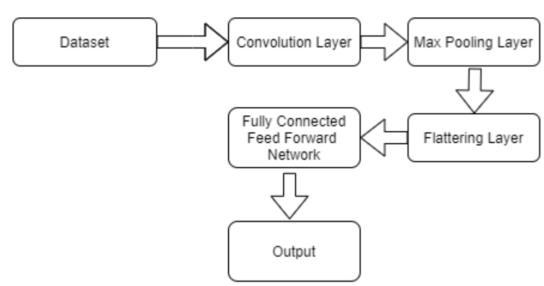

Fig. 4. CNN Model

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]. The aim of using multiple convolutional and pooling layers is to discover different scales of complex hierarchical features from the given data.

V. Evaluation and Performances

A. 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 results, classifying 8 types of attacks stated in dataset. While training the tuned model with best parameters found via GridSearchCV method as shown below, it is plotted with the parameters and how with every tuned model the CV score is improving leading to greater accuracy of the MLP model. The Graph is plotted as:

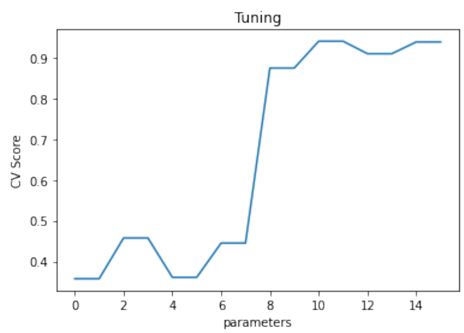

Fig. 5. Hyperparameter tuning in MLP

B. CNN

The CNN model implied in this paper is made up of two layers CONV1D i.e. convolution 1-D. Each layer is having pooling (downsampling) 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.

As the plotted graph below evident that the CNN model has resulted after training by projecting 94.43% validation

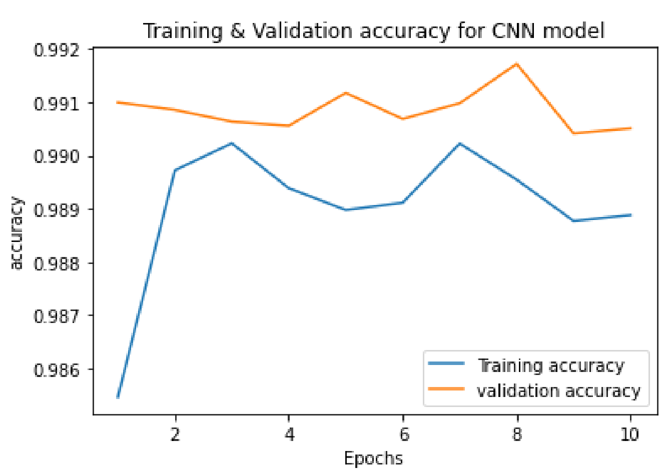

Fig. 6. Accuracy plotted for CNN

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 optimised 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. The last hidden layer is a fully connected layer that is flattened i.e, converts multi dimensional output array to one single dimensional array so as 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" activation function except the last classifying layer which has a sigmoid classification layer with dense output of 8 units since the dataset has 8 output labels for classification

C. LSTM

The plots shown by the LSTM model has the improvement of network modeling consequently by each epoch. It has been experimented with different batch sizes, epochs, layers. The results produced are found to be optimized for around 90.78% validation accuracy in total of 400 epochs. The above graphs show the accuracy is kept on increasing with the number of epochs and there is not much problem of over-fitting of the network. The fluctuations while training the model observed.

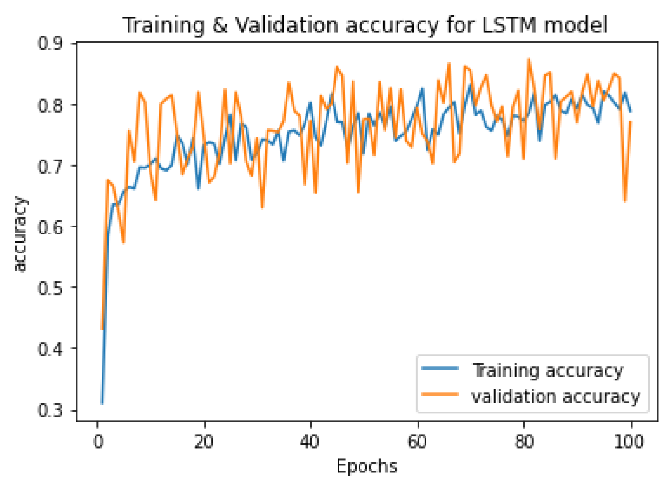

Fig. 7. Accuracy for MLP NN

The LSTM layer is comprising two layer, Layer-1 is the sequential model is designed with an LSTM layer of 100 LSTM units present in it. The layer is activated with relu as an activation function for all cells present in it. Whereas the Layer-2, The next layer used is 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 an 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.

VI. System Overview

The three proposed Deep Learning model were coded and compiled over Google's open source tool, named "Google Colab". The Google colab provides a free cloud service quite similar to Pycharm or Anaconda's Jupyter Notebooks supporting free GPU to research scholars like us. It has 2vCPU @ 2.2GHz, 13GB RAM, 100GB Free Space, which has stand by of 90 minutes with maximum 12 hours stragith run. The pro version lets you unlock this limits twice. The algorithms utilised Python3.6+ version and its libraries like Keras, Tensorflow, Pandas, sklearn, matplotlib et al

VII. Results and Experiment Analysis

The MLP has resulted a training accuracy of 95% while the validation accuracy is resulted 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 the precision, recall, f1 score macro averages are given as 95% each. Finally, the designed MLP neural network is able to detect the pattern in attacks that are observed in smart homes using IoT and concretely commits 95 out of 100 predictions correctly. The classification report and confusion matrix is shown below:

Classification Report

	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-FileDownload	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
FileDownload	1.00	1.00	1.00	20000
PartOfAHorizontalPortScan	0.85	0.77	0.81	20000
accuracy			0.95	160000
macro avg	0.95	0.95	0.95	160000
weighted avg	0.95	0.95	0.95	160000

Fig. 8. Classification Report for MLP NN

The other metrics like precision, recall, f1 score from the classification report are given as 96%, 94%, 94% respectively. The classification report can be conform the stated results

LSTM network has given very promising results with validation accuracy of 90.78% with a training accuracy of 86%. The difference between training and validation accuracy scores are in 5% range. This shows that the LSTM recurrent neural network is able to produce the same results on unknown data. The other results that are checked while evaluating the network

	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-FileDownload	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
FileDownload	1.00	1.00	1.00	20000
PartOfAHorizontalPortScan	0.98	0.60	0.74	20000
accuracy			0.94	160000
macro avg	0.96	0.94	0.94	160000
weighted avg	0.96	0.94	0.94	160000

Fig. 9. Classification Report for CNN

on test data of 20% available are precision, recall, f1 score which are produced as 91%, 91%, 90% respectively of macro averages and weighted averages. This shows the network is able to produce more than 90% accurate results on the IoT-23 smart home data available. The classification report is shown as below

	precision	recall	f1-score	support
Attack	0.99	1.00	0.99	20000
Benign	0.97	0.79	0.87	20000
C&C	0.75	0.95	0.84	20000
C&C-FileDownload	1.00	1.00	1.00	20000
C&C-Torii	0.90	0.98	0.94	20000
DDoS	0.90	0.99	0.95	20000
FileDownload	1.00	1.00	1.00	20000
PartOfAHorizontalPortScan	0.75	0.56	0.64	20000
accuracy			0.91	160000
macro avg	0.91	0.91	0.90	160000
weighted avg	0.91	0.91	0.90	160000

Fig. 10. Classification Report for LSTM

VIII. Future Work

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

IX. Conclusion

Three neural networks have been employed, MLP, CNN, and LSTM in order to complete the work This suggests that at least 90% of the attacks in the Internet of Things can be detected and categorised as belonging to one of 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 have the ability to identify breaches. The study can be generalised to incorporate other neural networks in the future.

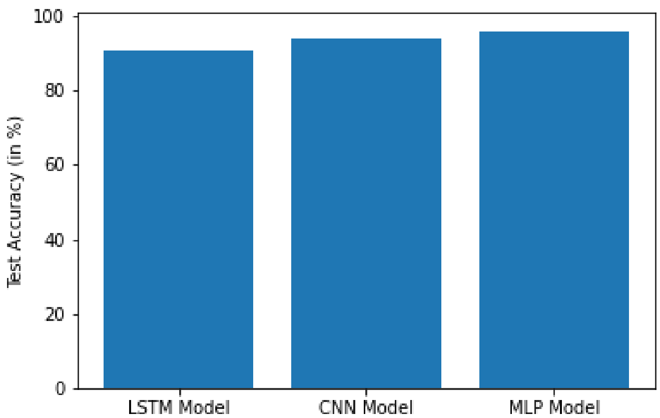

Fig. 11. Comparing DL models

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.