Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

# *Web Security in IoT Networks using Deep Learning Model*

Sanjay Patidar
Computer Science and Engineering Department
Delhi Technological University
New Delhi, India
sanjaypatidarcs@gmail.com

Inderpreet Singh Bains
Computer Science and Engineering Department
Delhi Technological University
New Delhi, India
inder.rockstar07@gmail.com

***Abstract*—The vision of IoT is to interface the things utilized in our day-to-day lives (which have the capacity of detecting and activation) via internet platform. This may or might possibly include humans. IoT field is developing and has many open digital issues. Internet of things (IoT) is still remaining in its early stages and has pulled in much enthusiasm for some mechanical parts including clinical fields, tech savvy, urban communities, and automotive. Anyway, as a paradigm, it is defenseless towards a scope of significant intrusion threats. In IoT whenever there is a web attack then it is required to remove the attack by installing software and so by using these models the attack can be removed from the system. This paper presents a threat investigation on IoT and utilizations on artificial neural network (ANN) to battle these threats. In this paper, profound learning method to incorporate digital security and prevention against attacks is also deployed, where a convolution 1d with multiple convolutions is used to increase the accuracy of the user. Profound models of learning are proposed and assessed those utilizing with the most recent CICIDS2017 datasets for DDoS assault recognition that has given most noteworthy precision of about 99.38%. It is essential to create an efficient intrusion identification framework that uses a deep learning mechanism to overcome attack issues in IoT framework. In this paper, a convolutional neural network [CNN] is developed with multiple convolution layers and accuracy of attack detection is also increased.**

***Keywords—CNN; attacks; IoT; threats; deep learning.***

## I. INTRODUCTION

### *A. IoT architecture*

The Internet of Things (IoT) is viewed as a future web that stretches out the internet to all way of genuinely shrewd gadgets in reality. A Cisco study reports the association between these brilliant gadgets and the Internet by around 50 billion constantly 2020. [1] The Internet of Things (IoT) is viewed as a future internet which stretches out the internet to all way of truly shrewd gadgets in reality. [2] IoT will give the wise and self-created cyberphysical frameworks in the fields of clever lattices, savvy urban communities, lodging, wise clinical and clinical administrations, wearable advancements, travel frameworks, and so on., by connecting these billion brilliant gadgets to the Internet. [3] The main work under IoT is for cyber security. Web of Thing is the most recent rising and encouraging innovation that interfaces everything across the globe through web. IoT innovation assures to enhance and support our own, proficient life and culture [4]. IoT comprises of a system of brilliant protests that are spread far and wide through internet with no human obstruction, which is incredible yet it is powerless to digital assaults like some more system. [5]The security of IoT framework is a significant test in modernization. [6] While many existing arrangements depend on human-characterized highlights to create AI (ML) based attack finders against noticeable adventures, such highlights are turning out to be progressively costly and less compelling in the smart network. [7]

The client's unit handles significant security-situated by taking care of frameworks entirely for information security. For example, encoding, unscrambling, and protection order forms. In IoT, these computationally escalated exercises can't be dealt by asset constrained keen machines as a wellbeing focused tasks that support the noisy computing strain. [8]One of the significant difficulties in cybersecurity is the arrangement of a robotized and compelling cyber-threats identification procedure. To overcome this difficulty, deep learning techniques are generally used in cyber security. [9] For this, several intrusion detection systems are implemented, which can check if any attack happens under software layers.

An important technique for detecting cyberattacks in any network is the intrusion detection system (IDS). A considerable lot of the new IDS depend on network-based AI algorithms to train and detect cyberattacks. Fog computing is an improved augmentation of brought together distributed computing wherein disseminated mist hubs are nearer to IoT arrange articles and address adaptability congestion, high data transmission usage nature of administration humbling, and minimal cloud computing high inertness. Fog-to-node registering is suitable for IoT networks being deployed in operation and being efficient. The figure below illustrates the haze to-hub model architecture with appropriated equal calculation giving insight to the disseminated hazes by giving IDS closer to the IoT organize objects computation, control, and storage. In this IoT networks are created which has fog, and has IDS which detects the attacks from users before connecting to the cloud. Compared with the cloud, IDS detect cyber threats easily and rapidly at fog nodes. IoT network consists of links between various types of savvy objects going from supercomputers to minuscule gadgets, which may have low processing capacity, so it is difficult to access these types of networks. Therefore, cybersecurity is a significant shortcoming in IoT network implementation. [10]

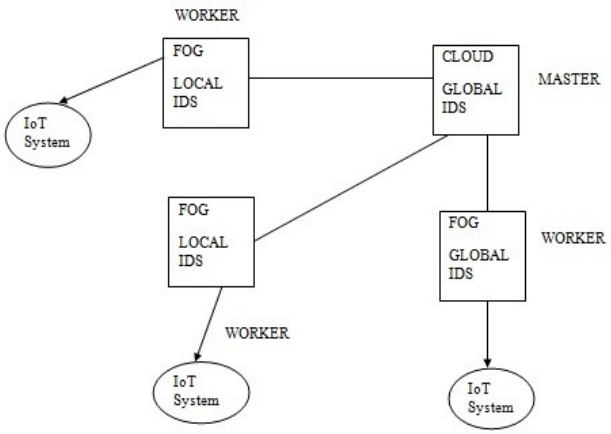


Fig. 1. IoT network architecture

### *B. CNN Methodology*

Using the convolutional operation on the input datasets with pre processing and special layers and filters are applied in CNN method. Fig. 2 shows the base model representation of the CNN based model. The input data sets are fed using their features. Then convolution operation is applied. Maxpool, dropout and fully connected layer parts of CNN methodology is applied for the final output through dense layers. In this methodology convolutional layers are considered; however, will make it deeper by adding more convolutional layers, as well as maxpooling layers. Max pooling layer is included to dispose of highlights with low score and keep just highlights with most elevated score. The outcomes are down tested or pooled include maps that feature the most present component in the fix. This has been found to work preferred by and by over normal pooling for PC vision errands like picture arrangement. Dropout layer is added to spare framework from warming. Yield from the dropout layer is taken care of to completely associated layer which then give contribution to the thick bed alongside sigmoid capacity.

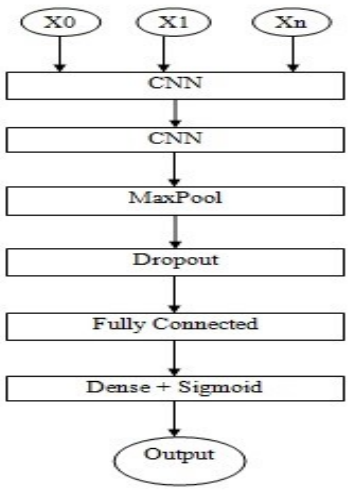


Fig. 2. CNN methodology

This paper is composed as follows: in section II, background work is mentioned. In section III, literature of previous year papers and existing information about IOT in brief is mentioned. In the section proposed IV work is presented. In section V implementation of approach of deep learning in cyber security for IOT is presented. Finally, in the next section results are shown and concluded the paper

## II. BACKGROUND

The configuration of the 1D deep CNN model consists of an information layer, a convolutional layer, a max pooling layer, a completely associated layer, and a yield layer as shown in figure 3. We have applied a 1D Convolutional Neural Network on our data. A 1D CNN is exceptionally successful when you would like to get intriguing features from shorter (fixed-length) portions of the general educational record and where the territory of the component inside the area isn't of high significance. This applies well to the examination of time successions of sensor information. It additionally applies to the investigation of any sort of sign information over a fixed-length period, (for example, sound signs). Another application is NLP.

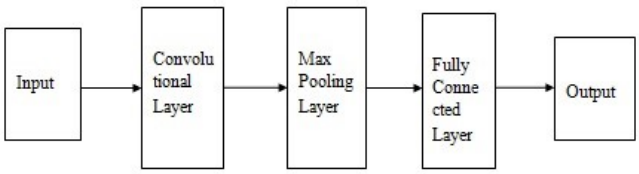


Fig. 3. 1d CNN architecture

## III. LITERATURE REVIEW

### *A. The Internet of Things*

The Internet of Things (IoT) as an idea has its roots in the early 1990s was likely one of the first people to recognize the eventual rise of a system where on-demand computing was available to everyone through a combination of hardware and software, connected using wires or radio communication. N.Y. Parotkin et al. [11] in modern times, this idea has materialized as a viable and imminent future technology, characterized by a massively connected system of items or devices which can associate with each another over a network connection.

R. Mahmoud et al. [12] today's widespread, worldwide telecommunications network lays the foundation for massive IoT in the near future. The rise of IoT as a technology platform is also partially attributable to the rapid downward scaling (miniaturization) of transistors; a trend that has been fairly consistent since the late 20$^{th}$ century and continues into the 21$^{st}$ century. Transistors form the bedrock of all silicon-based intelligence in today's time. This observed law of miniaturization is well documented in Dennard's Scaling and Moore's Law; two well-known observations relating to computing in recent times. Current advances in miniaturization allow small sensors and computing modules to operate cheaply, efficiently, and be deployed at a large scale across a wide range of real-world applications.

The Industrial applications of IoT (IoT) are of particular interest to this paper. IoT devices are primarily used to ingest and analyses data from industrial equipment, operational technology, physical locations, and human resources. Cyber security is an intensive industrial activity in the modern world; given its essential nature, IoT can make significant improvements to it. [13]

### *B. Deep Learning Methods for Security in IOT*

Subsequently, our exploration work advocates improving IoT security by utilizing Deep Learning calculations. W. Abbass et al. [14] Deep Learning is in no way, shape or form an ongoing worldview. It is a subfield pertaining to machine training that has its underlying foundations in Artificial Intelligence. Profound Learning helps essentially perform characterization assignments straightforwardly from writings, pictures and sounds. As of now, Deep Learning is to a great extent engaging the IT scene by tackling different issues. The neurons of the ANN are utilized to form complex hypotheses; the more neurons, the progressively complex the speculations. Assessing the speculations is finished by setting the info hubs in a criticism procedure and the occasion streams are spread through the network to the yield where it is named typical or bargained. J. Lee et al. [15] at this stage the inclination plunges are utilized to push the blunder in the yield hub back through the network by a back-proliferation process so as to gauge the mistake in the concealed hubs. The inclination of the expense – capacity would thus be able to be determined [16]. Neural network framework experiences preparing so as to gain proficiency with the example made in the framework. There are many techniques applied in cyber security with the help deep learning. Some of the techniques are LTSM which long term short memory. Recurrent neural network known as RNN is used in some papers. Also, some researchers have used natural language processing techniques and support vector machine is also used.

Subsequently, different systems like convolutional neural networks are likewise effectively investigated around there, which incorporates input surface, convolution surface, pooling surface, completely associated surface, and yield surface. Konstantinos P. Ferentinos [17] discusses plant disease detection and diagnosis models through a database that contains photographs of healthy and infected plant leaves. The future direction in this is to gather a wide range of training data from various sources from different geographic areas, conditions of cultivation, and other factors.

In SenseBox architecture, H M Sajjad Hossain et al. [18] proposed a DeActive model. This algorithm is executed much more quickly than other algorithms. Dynamic learning can assist us with alleviating the manual effort expected to compile ground-level data about truth and decrease preparing time. With far less marked cases, DeActive can give better precision, which also ensures lower annotation effort.

Chris Xiaoxuan Lu et al. [19] examined security aspects by sniffing a deep learning smartwatch password that is a Snoopy method. Snoopy uses a uniform structure to separate movement information portions, albeit passwords are inserted, and utilizes new profound neurological systems directed toward surmise the real watchwords. This system can effectively spy information on moving out of sight while entering passwords. Without devouring noteworthy force/ computational assets, it can successfully extract password segments of motion data on smartwatches in real-time.

Parisa Pouladzadeh et al. [20] presented an app that utilizes the image of the nourishment, taken by the client's cell phone, to perceive different nourishment things in a similar food to evaluate the calorie and sustenance of the nourishment. In this, the client is challenged to rapidly recognize the broad territory of nourishment by an outline a bouncing ring on the nourishment image by contacting the canopy. The framework, at that point, utilizes picture handling and statistical insight for food item acknowledgment.

Jennifer S. Raj et al. [21] introduced a study of the computational smart strategies as they appear to be viable option for the man-made brainpower by conquering the disappointments and disadvantages in it. Examination of the different computational strategies to locate the ideal one in the identification of false access will be a future heading.

Samuel Manoharan et al. [22] introduced measures to improve the likelihood of the wellbeing for the vehicles with the capacity of self driving worked with man-made reasoning empowered processors. Further the model guaranteed the ability of the security calculation in oneself driving vehicles.

## IV. PROPOSED WORK

In this section, detailed methodology and proposed models are explained. The main objectives are to implement deep learning method with higher accuracy in cyber security to compare the accuracy with existing methods.

### *A. Proposed Methodology*

The flow diagram of our framework is shown in figure 4; here the input is the csv files which were gathered with several diverse digital assaults alongside with usual data for five consecutive days. In this, first applied the convolution 1d to our system and then divide the dataset into two categories: BENIGN and Web attack. BENIGN is neural and rest are different web attacks Then in the next step label the data by assigning benign as 0 and web attack as 1. Then divide the information into 70% preparing as well as 30% for examination. Then set the batch size to 32 and epoch which are the number of rounds to 100. Then use for loop for epoch=1, 2, 3 and so on. For this set the count to 0 and repeat until count+batch size< no. of training samples else it goes back to the dataset division. Then train the classifier on benign and web attack to help him learn to classify different web attacks, and then set count equal to batch size and then perform testing on benign and web attack. The last step which is the output is to compute the exactness, accuracy, recall and f1-score from the confusion matrix to know the accuracy of model.

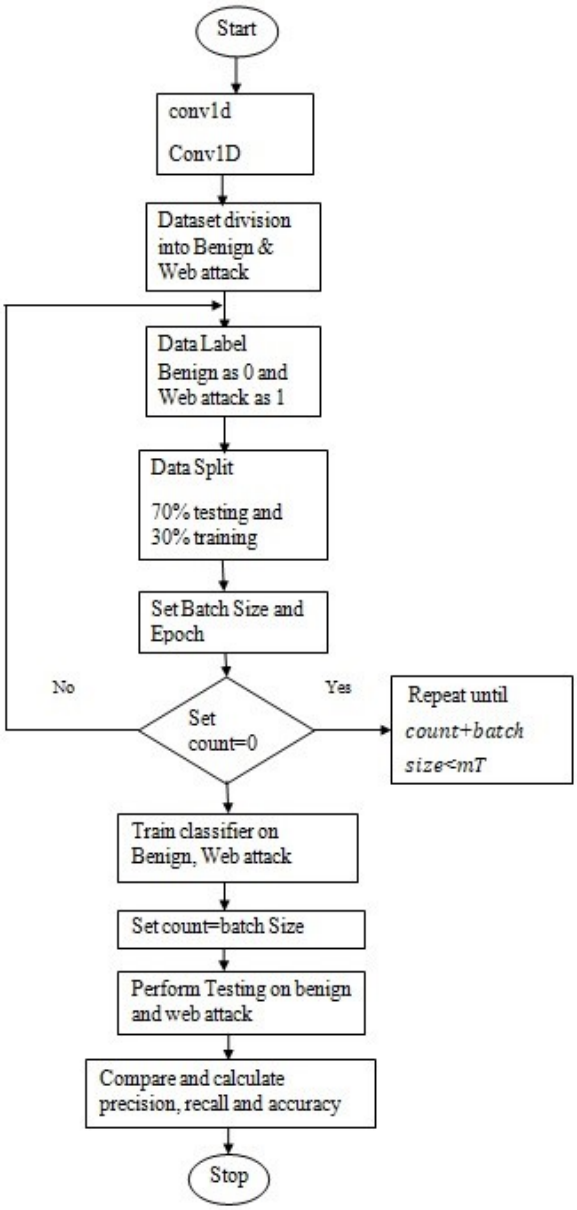


Fig. 4. Proposed Methodology

*B. Algorithm*

The proposed algorithm is given below:

**Input:** $m$- No. of samples
$n$- No. of features
0- Label for BENIGN data
1- Label for Web attack
$mT$- No. of training samples
$mt$- No. of testing samples
$XTmT\times n$- Training samples
$YTmT\times 1$- Training labels
$Xtmt\times n$- Testing samples
$Ytmt\times 1$- Testing labels
$Ypredmt\times 1$- Predicted labels
**Output:** tp, tn, fp, fn

1. Prepared dataset $Xm\times n$ and label $Ym\times 1$ where $Y\in \{0, 1\}$
2. Split data $Xm\times n$ and label $Yn\times 1$ into 70% training and 30% testing sets
3. $(XTmT\times n,\times 1)$ is the training set and $(Xtmt\times n,Ytmt\times 1)$ is the testing set
4. Set $batch\ \ size$=512 $and\ epoch\ s$=100
5. for $epoch$ =1,2,3,……..,$epoch\ s$
6. Set $count$=0
7. Repeat until $count$+$batch\ \ size$<$mT$. Train classifier on (XT$count$+1 $to\ \ count$+$batch\ \ size$, YT$count$+1 $to\ \ count$+$batch\ \ size$)
6. Calculate accuracy
7. Set $count$=$batch\ \ size$
8. end for
9. Perform testing on $Xtmt\times n$ and find $Ypredmt\times 1$
10. Compare $Ypredmt\times 1$ and $Ytmt\times 1$ and calculate precision, recall, F1-Score, Accuracy

First, divide the information into the preparation and testing part, where 70% of data have utilized for preparing and rest 30% part for testing. Since, the dataset is highly imbalanced, where attacks are in minimum quantity as compared to the BENIGN. Therefore, a different strategy such as multilevel classification can be adopted where the first decision will be whether the data is BENIGN or ATTACKED. If data comes in ATTACKED category then will predict the nature of the attack. Then set the batch size to 512 and epoch which are the number of rounds to 100. Then use for loop for epoch=1, 2, 3 and so on. For this set the count to 0 and repeat until count+batch size< no. of training samples else it goes back to the dataset division. Then train the classifier on benign and web attack and then set count=batch size and then perform testing on benign and web attack. The last step is to compute the exactness, accuracy, recall and f1-score from the confusion matrix to know the accuracy of model.

*C. Proposed CNN 3 Layer Model*

The proposed model 1 also known as CNN 3 layers is used, which is the modified CNN based deep learning algorithm as shown in the figure 5. In this figure, multiple layers of deep learning-based convolution and max pooling are applied to improve the accuracy. In this there are convolution bed followed by max pooling bed after that dropout layer is applied. The dropout layers are combined to spare the framework from warming. Yield from the dropout layer is taken care of to flatten bed which at that point provide input for the dense bed which then provide input to the subsequent dropout layer. Yield from the dropout bed is taken care of to the second dense layer with sigmoid, relu, and softmax activation function. This CNN model is ideal when requirement is of less computation as there is less parameter required in this model. Here the accuracy of the model is 99.10%.

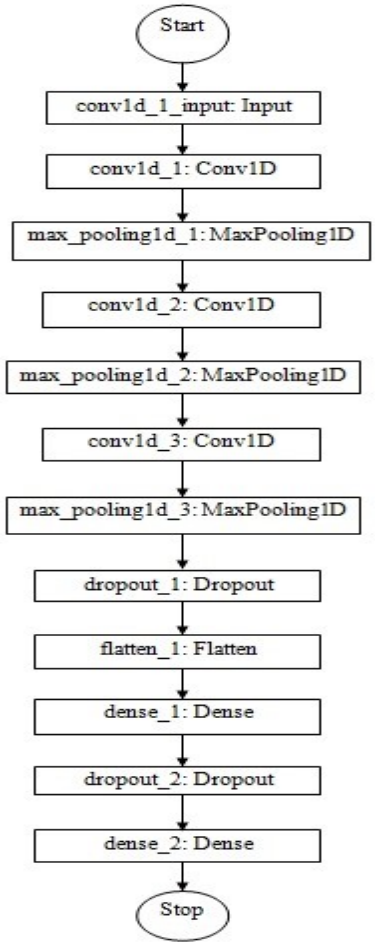


Fig. 5. Proposed CNN 3 Layer Model

### *D. Proposed Multiheaded CNN Layer Model*

The proposed model 2 also known as multiheaded CNN layers is used, which basically concatenate three CNN processes as shown in the figure 6. They are followed by maxpooling layers, dropout layers and flatten layers and then it connects them with concatenate layer. Yield from the concatenate layer is connected to the dense bed that gives contribution to the dropout bed. The dropout bed is added to spare framework from warming. Yield from the dropout bed is connected to the second dense bed with sigmoid, relu, and softmax activation function. In this model the layers are connected parallelly which is why this model is also known as multiheaded CNN layers. It gives significant improvement in the accuracy and other measures as it applies multiple CNN layers to reduce the error to minimum. This CNN model is ideal when requirement is of high computation as it requires more parameters. Here the accuracy of the model is 99.38% which is the highest of all the models.

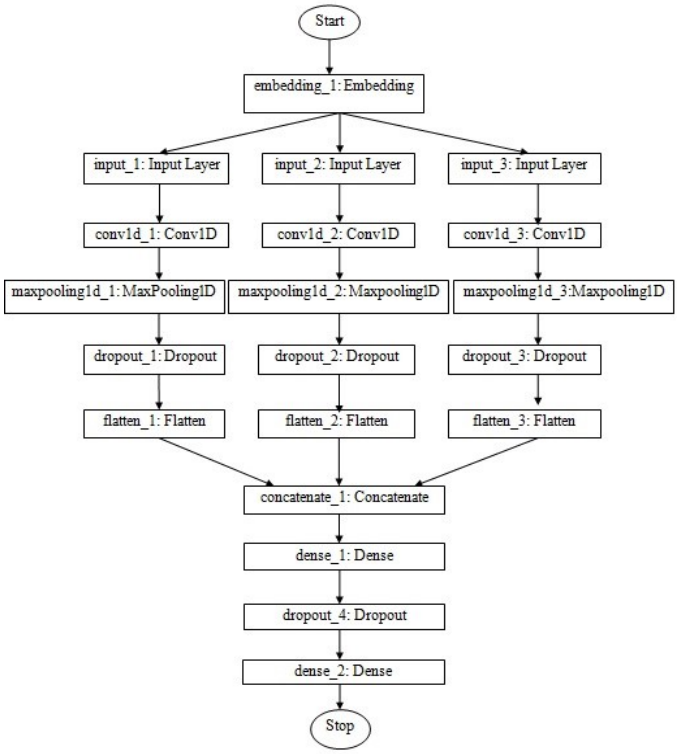


Fig. 6. Proposed Multiheaded CNN Layer Model

## V. IMPLEMENTATION

In this segment first we illustrated the experimental setup and then the dataset used in the paper.

### *A. Experimental Setup*

This work is utilized by using Keras [23] on Tensorflow bundle for profound study on 64-bit Intel core-i5 CPU with 30 GB RAM in Windows 7 environment. In this there are local parameters and global variables.

**Local parameter**

Local parameters are announced within a function and can be utilized distinctly inside that function. Local variables of the same name can be used in different functions. Local parameters in this are: number of features, label for benign, label for web attack, number of training samples, training samples, testing samples, training labels, testing labels, predicted labels, true positive, true negative, false positive, false negative.

**Global parameter**

Global parameters are announced outside any function, and they can be utilized on any capacity in the program.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F - Measure = \frac{2 * Precision * Recall}{Precision + Recall} \quad (4)$$

In this, TP is genuine positive, FN is bogus negative, TN is genuine negative and FP is bogus positive. F1 score depends on precision and recall. Since the dataset is imbalanced, therefore the exhibition of the models is assessed as far as Precision, Recall, F1-Score, and Accuracy.

### B. Dataset

For leading proposed work we have utilized most recent DDoS assault CICIDS2017 dataset. CICIDS2017 datasets contain exceptional genuine work arrange taking after information. This dataset was accumulated for 5 sequential days with different cyberattacks alongside ordinary information. This dataset contains latest cutting-edge arrange information with and without assault which is near the genuine work organize data.

In this implementation, python language is used. There are 2830743 data samples and 79 features. After preprocessing like removing columns having all zeros and normalization, we have total 76 features.

In this implementation, further we will discuss about the dataset. It contains total 2830743 data samples from 15 different categories having 79 features. The categories and the percentage of data samples in the dataset are as follows: BENIGN (80.3%), Infiltration (0.0013%), DDoS (4.52%), Bot (0.069%), Web assault sql infusion (0.0007%), SSH-Patarator (0.21%), DoS slowloris (0.20%), DoS Hulk (8.16%), PortScan (5.61%), Heartbleed (0.0004%), DoS Slowhttptest (0.19%), DoS GoldenEye (0.36%), FTP-Patarator (0.28%), Web assault Brute Force (0.053%), Web assault XSS (0.023%).

Out of 15 categories BENIGN is neural and rest are different web attacks. As we can see that percentage of individual attacks data in many cases are around 0%. BENIGN is the most used data sample in the dataset with the second being DoS Hulk. Therefore, we have divided data into two parts BENIGN and Web Attacks and then profound learning models are applied to arrange the information into either of the two categories. The dataset contains 79 features, some of highlights are: goal port, stream duration, aggregate forward parcels, complete in reverse bundles, absolute length of forward bundles, all out length of in reverse bundles, forward bundle length max, forward bundle length min, forward parcel length mean, forward parcel length standard, backward parcel length max, backward parcel length min, backward bundle length mean, backward bundle length standard, stream byte/s, stream packet/s, stream IAT mean, stream IAT standard, stream IAT max, stream IAT min and so on.

## VI. RESULTS

In this section, results are presented. The testing of results is done in complete week bases with different attacks and methods on each day. The results are basically comparison of the performance metrics explained in previous section. The exhibition of the classifier is presented in Table 1. The performance metrics are then analyzed for each of the models and further explained in results section.

The confusion matrix for all the models is presented in figure 7, 8, and 9. From this we can get the values of genuine positive, genuine negative, bogus positive, bogus negative and ascertain exactness, recall, along with precision.

### A. Confusion matrix of CNN Model

The disarray network of the CNN model which is the base model is shown in figure 7. For example Heartbleed attack 100% incorrectly classifies the attack as BENIGN. However the second attack DoS slowloris 97% correctly classifies that the attack is DoS Slowloris but 2 % incorrectly the attack as BENIGN and DoS Slowhttptest. Similarly we calculate the values of all attacks and then calculate the accuracy recall, precision of the model.

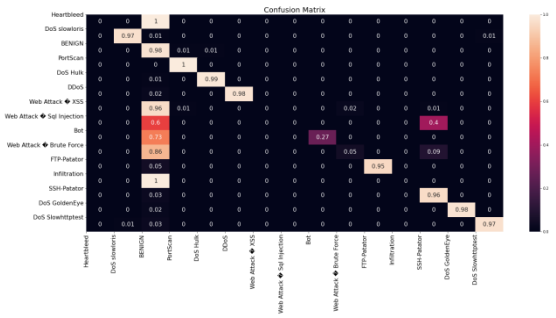


Fig. 7. Confusion matrix of CNN model

### B. Confusion matrix of Proposed CNN 3 Layer Model

The disarray network of the proposed CNN 3 layer model is shown in figure 8. For example Web attack-brute force attack does not correctly classifies that it is the same attack. Instead it 92% incorrectly classifies the attack as BENIGN. Similarly the second attack Web attack- XSS 99% incorrectly classifies that the attack is BENIGN. Similarly we calculate the values of all attacks and then calculate the accuracy recall, precision of the model.

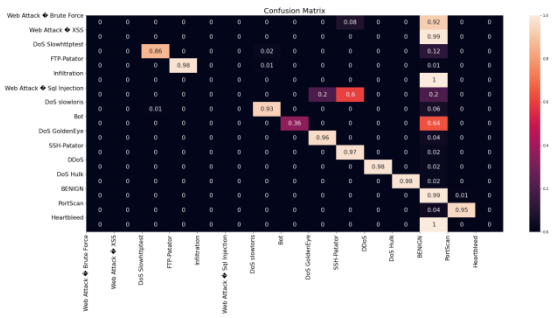


Fig. 8. Confusion matrix of proposed CNN 3 layer model

### C. *Confusion matrix of Proposed Multiheaded CNN Layer Model*

The disarray network of the proposed multiheaded CNN layer model is shown in figure 9. For example Heartbleed 100% incorrectly classifies the attack as BENIGN. The second attack SSH-patator 97% correctly classifies the attack as SSH-patator but 3% incorrectly classifies the attack as BENIGN. Similarly we calculate the values of all attacks and then calculate the accuracy recall, precision of the model.

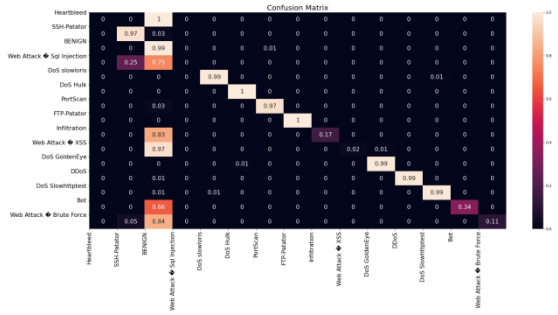


Fig. 9. Confusion matrix of proposed multiheaded CNN layer model

### D. *Performance Metrics Evaluation*

The performance metrics evaluation is shown in table 1. In this the CNN model has precision of 94.33%, recall of 97.62%, f1-score of 96.41%, and accuracy of 98.32%. The second model which is the proposed CNN 3 layer model has precision of 96.54%, recall of 98.44%, f1-score of 97.48%, and accuracy of 99.10%. The third model which is the proposed multiheaded CNN layer model has precision of 98.70%, recall of 99.33%, f1-score of 99.01%, and has an accuracy of 99.38% which is the highest of all the models.

Table I. Performance Metrics Evaluation

| Model Name | Precision | Recall | F1-Score | Accuracy |
|---|---|---|---|---|
| CNN Model | 94.33 % | 97.62 % | 96.41 % | 98.32 % |
| Proposed CNN 3 Layer | 96.54 % | 98.44 % | 97.48 % | 99.10 % |
| Proposed Multiheaded CNN Layer | 98.70 % | 99.33 % | 99.01 % | 99.38 % |

The epochs vs. accuracy and epochs vs. loss chart for all models are presented in Figure 10, 11, and 12.

### E. *Epoch vs. Accuracy and Epoch vs. Loss curve of CNN Model*

In this CNN model the testing accuracy versus epoch is significantly high in the below figure 10 for the first model. As we increase the number of epochs the testing accuracy also increases. Here epochs are the number of rounds in which we are running the model. The loss vs. epoch curve shows that loss is decreasing as the number of rounds increases.

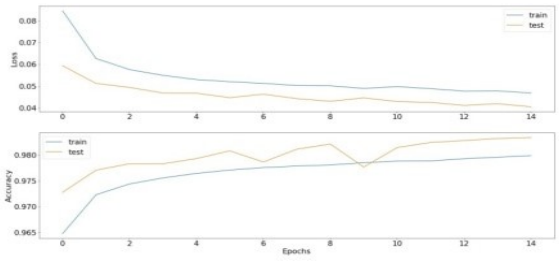


Fig.10. Epochs vs. Accuracy and Epochs vs. Loss curve of CNN Model

### F. *Epoch vs. Accuracy and Epoch vs. Loss curve of Proposed CNN 3 Layer Model*

The CNN 3 layer model for the representation results is shown in figure 11; variation in accuracies is seen as per the increase in the epochs. As number of rounds increases there are variations in testing accuracy. The variation in accuracy shows that the accuracy is not constant it keeps on fluctuating. The loss vs. epoch curve shows variation in loss as per the increase in the epochs.

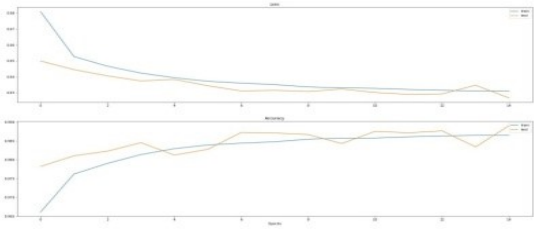

Fig. 11. Epochs vs. Accuracy and Epochs vs. Loss curve of proposed CNN 3 layer model

### G. *Epoch vs. Accuracy and Epoch vs. Loss curve of Proposed Multiheaded CNN Layer Model*

The final proposed multiheaded CNN model result for accuracy and loss curve is seen as shown in figure 12, which improved in terms of high accuracy and low loss techniques result. In this the testing accuracy is improved in terms of low loss in the model. The loss vs. epoch curve shows loss is decreasing and as a result testing accuracy of the model increases. This model has the highest accuracy as compared to the rest of the models.

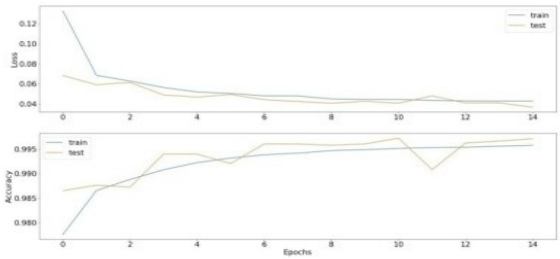


Fig. 12. Epochs vs. Accuracy and Epochs vs. Loss curve of proposed multiheaded CNN layer model

### H. *Comparison of Evaluation parameters for all models*

Comparison of all three-model implementation on the basis of four parameters, accuracy, F1 score, recall and precision are

shown in figure 13 for deep learning method in cyber security. Here model 1 is the cnn model which is the base model, model 2 is the proposed cnn 3 layer model, and model 3 is the proposed multiheaded cnn layer model. It is seen that proposed multiheaded cnn layer model is the best amongst the others and has a higher accuracy amongst all that means has the least error.

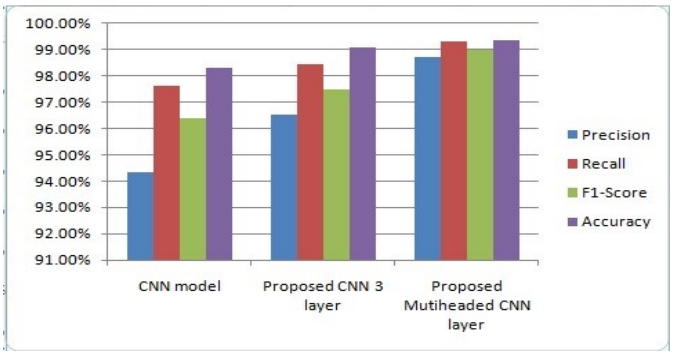


Fig. 13. Comparison of evaluation parameters for all models

## VII. CONCLUSION

Web of Thing is the most recent significant development that interfaces all around the globe through web. IoT development helps to improve and bolster the proficient lifestyle and culture. The proposed work is focused on deep learning innovation using CNN and its different model variants. The datasets are used and tested with all possibilities to give better results and innovation in cyber security issues for internet of things. The loss and accuracy are the main parameter for analysis in the ground pertaining to security improvement under the web of things domain. Hence, this paper has provided an improved method to detect security issues in IoT by using a modified deep learning method. The proposed results indicate a higher accuracy in the CNN modified algorithm. In future it can be tested on edge servers and cloud assisted servers. As it is highly unbalanced by duplicating data, the dataset is balanced for this study; this could be enhanced in the future by developing a deep learning model that could run on the unbalanced dataset.

## REFERENCES

[1] M. Roopak, G. Yun Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2019, pp. 0452-0457, doi: 10.1109/CCWC.2019.8666588.

[2] Thamilarasu, Geethapriya & Chawla, Shiven. (2019). Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. Sensors. 19. 1977. 10.3390/s19091977.

[3] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 315-318, doi: 10.1109/ICICCS.2016.7542301.

[4] A. Samandari, M. Ge, J. B. Hong and D. S. Kim, "Evaluating the Security of IoT Networks with Mobile Devices," *2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, Taipei, Taiwan, 2018, pp. 171-180, doi: 10.1109/PRDC.2018.00028

[5] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769560.

[6] A. Aldaej, "Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI)," in *IEEE Access*, doi: 10.1109/ACCESS.2019.2893445.

[7] F. Ullah *et al.*, "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," in *IEEE Access*, vol. 7, pp. 124379-124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[8] F. Rahman, M. Farmani, M. Tehranipoor and Y. Jin, "Hardware-Assisted Cybersecurity for IoT Devices," *2017 18th International Workshop on Microprocessor and SOC Test and Verification (MTV)*, Austin, TX, 2017, pp. 51-56, doi: 10.1109/MTV.2017.16

[9] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103-2115, April 2019, doi: 10.1109/JIOT.2018.2869847.

[10] A. Chadd, "DDoS attacks: past, present and future," *Network Security,* vol. 2018, pp. 13-15, 2018.

[11] N. Y. Parotkin and V. V. Zolotarev, "Information Security of IoT Wireless Segment," *2018 Global Smart Industry Conference (GloSIC)*, Chelyabinsk, 2018, pp. 1-7, doi: 10.1109/GloSIC.2018.8570144.

[12] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[13] M. R. Schurgot, D. A. Shinberg and L. G. Greenwald, "Experiments with security and privacy in IoT networks," "*2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston, MA, 2015, pp. 1-6, doi: 10.1109/WoWMoM.2015.7158207".

[14] W. ABBASS, Z. BAKRAOUY, A. BAINA and M. BELLAFKIH, "Classifying IoT security risks using Deep Learning algorithms," 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 2018, pp. 1-6, doi: 10.1109/WINCOM.2018.8629709.

[15] J. Lee, J. Kim, I. Kim and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," in *IEEE Access*, vol. 7, pp. 165607-165626, 2019, doi: 10.1109/ACCESS.2019.2953095.

[16] D. Wilson, Y. Tang, J. Yan and Z. Lu, "Deep Learning-Aided Cyber-Attack Detection in Power Transmission Systems," *2018 IEEE Power & Energy Society General Meeting (PESGM)*, Portland, OR, 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8586334.

[17] Dan, C., Meier, U., Masci, J., Gambardella, L.M., Schmidhuber, J. "Flexible, high execution convolutional neural systems for image classification," Events of the 22nd International Joint Conference on Artificial Intelligence, vol. 2, pp. 1237–1242, 2011.

[18] Hande Alemdar, TLM van Kasteren, and Cem Ersoy, "Active learning with ambiguity sampling for broad-scale activity identification in a smart dormitory," Journal of Ambient Intelligence and Smart Environments 9, 2, 209-223, 2017.

[19] Mariamn Harbach, Alexander De Luca, and Serge Egelman, "The anatomy of smartphone unlocking: A field study of android lockscreens" In ACM Conference on Human Factors in Computing Systems, CHI, 2016.

[20] Parisa Pouladzadeh, Pallavi Kuhad, Sri Vijay Bharat Peddi, Abdulsalam Yassine, and Shervin shirmohammadi. "Calorie measurement and food classification using deep learning neural network," in Proceedings of the IEEE International Conference on Instrumentation and Measurement Technology, 2016.

[21] Raj, Jennifer S. "A Comprehensive Survey On The Computational Intelligence Techniques And Its Applications." Journal of ISMAC 1, no. 03 (2019): 147-159.

[22] Manoharan, S. (2019). "An Improved Safety Algorithm For Artificial Intelligence Enabled Processors In Self Driving Cars",Journal of Artificial Intelligence, 1(02), 95-104.

[23] Keras deep learning P.W.D. Charles Project Title Available: https://github.com/charlespwd/project-title