Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 29, Issue 1 – March 2023

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

UGC CARE II

Framework for Improving Security and Resilience of IoT Networks

Smt Sampatkumari M B
Assistant professor
Govt. First Grade College Humnabad
Email: sampatmalkapure@yahoo.com

Abstract-

The Internet of Things (IoT) is being used in nearly every sector of society, from education and entertainment to the health care system and smart cities. Due to the widespread use of the IoT, organizations should concentrate their efforts on system security. Any vulnerability could lead to a system failure or cyberattack, which would have a large-scale impact. IoT security is a protection strategy and defense mechanism that protects against the possibility of cyberattacks that specifically target physically linked IoT devices. IoT security teams are currently dealing with growing difficulties, such as inventories, operations, diversity, ownership, data volume, threats, etc. Data integrity, secrecy, authentication, and authorization should be guaranteed due to the large amount of data that flows across network devices. However, the area of IoT security still has a lot of room for growth. The security of IoT systems is not alone endangered by Internet-connected Things, but the total environment, which includes websites, applications, social forums, and servers, is controlled by smart devices called robot networks.

Keywords— Internet of Things, Security, Network

I. INTRODUCTION

The third revolution in industries is said to be caused by the invention of the IoT [1]. The definition of an IoT device states that "it is a device interconnected with the internet embedded in objects used in day-to-day life for transmitting and receiving information" [2]. From 2006 to 2021, IoT demand has risen from 2 billion to 200 billion objects. Several encounters are confronted by specific events and environments using spatial and temporal information collected and processed frequently by IoT sensors and devices [3]. IoT objects' and things' behaviour has significantly improved in terms of elegance and intelligence, and communications have improved as well. As a result, IoT devices are used in almost every sector, such as logistics, green infrastructure, tourism, education, distributed energy resources, financial management, and even domestic and recreational activities [4].

The world has encountered a few critical specialized headways in PC organizing during the twenty-first 100 years, which is known as the time of remote correspondence and interconnectivity. Kevin Ashton previously utilized the expression " IoT" in 1999 [5]. IoT is a new innovation that empowers the improvement of organizations associating different things, whether in reality or the computerized one [2]. IoT gadgets, which range in size from small wearables to monstrous hardware and are equipped with actuators and sensors, can wisely detect their surroundings and make a move all alone [3,4].

Because more industries are utilizing IoT apps, the number of IoT applications and devices will rise. Wearable innovation with gadgets to screen and share an individual's way of behaving and wellbeing data is one such business that is giving wearable innovation. In the healthcare sector, IoT devices and apps are being made available to patients [5]. Presently accessible "savvy house" IoT items incorporate shrewd coolers, brilliant warming, shrewd cultivating, video doorbells, individual aides for brilliant lights, shrewd espresso producers, and savvy entryway locks. Savvy stopping, brilliant streetlamps, and shrewd junk the board are a portion of the "shrewd city" applications and IoT contraptions that have been created [6].

The academic community has shown a lot of interest in IoT security. The security of IoT gadgets has been an interesting issue among scholastics [7]. IoT has a lot going for it, but it also has three main issues: information transmission, information social affair, and information security. Many following applications have been made explicitly to gather information from IoT gadgets. Thanks to a variety of protocols that have been developed and modified to transmit gathered data, IoT devices can connect to existing networks and exchange data. In any case, they don't offer these conventions the consideration they require. Thus, IoT is firmly connected to numerous advanced and customary security issues, including recognizable proof, information security, consent, and so forth. Refusal of administration attacks, replay assaults, Denning-Sacco assaults, secret phrase speculating assaults, and so on. can all outcome from login defects. Then again, validating IoT gadgets across heterogeneous and connected networks is undeniably challenging. IoT device limitations, energy consumption, limited memory space, and limited computing power should also be taken into account by these protocols [8].

II. INTERNET OF THINGS

The Internet of things (IoT) is the network of devices such as vehicles, and home appliances that contain electronics, software, sensors, actuators, and connectivity which allows these things to connect, interact and exchange data. The IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled.

The idea of inter-connected is devices where the devices are smart enough to share information with us, to cloud based applications and to each other (device to device) [6].

Smart devices or “Connected devices” as commonly called as, are designed in such a way that they capture and utilize every bit of data which you share or use in everyday life. And these devices will use this data to interact with you on daily basis and complete tasks.

The Internet of Things refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems [7].

IoT Extends Internet Connectivity**:** The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smart phone sand tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet [8].

IoT Examples: Examples of objects that can fall into the scope of Internet of Things include connected security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more. Businesses can leverage IoT applications to automate safety tasks (for example, notify authorities when a fire extinguisher in the building is blocked) to performing real-world A/B testing using networked cameras and sensors to detect how customers engage with products [9].

The Future of IoT; As far as the reach of the Internet of Things, there are more than 12 billion devices that can currently connect to the Internet, and researchers at IDC estimate that by 2020 there will be 26 times more connected things than people. According to Gartner, consumer applications will drive the number of connected things, while enterprise will account for most of the revenue. IoT adoption is growing, with manufacturing and utilities estimated to have the largest installed base of Things by 2020 [10].

III. METHODOLOGY

IoT has developed as a unique skeleton/model of WSN in the last decade. Blue WSNs face difficulties that limit their capabilities. They necessitate specific customization for certain applications, making them more challenging to deploy and limiting their management and flexibility. SD-IoT is made by putting together the best parts of SDNs and WSNs to get around this problem. Moreover, SDN-WSN is susceptible to security risks, which has a detrimental impact on the system's performance and QoS vulnerability. System unreliability would occur from DoS/malicious attacks, for instance those employing fictitious data and settings [11]. As a result, the massive installation of WSNs is difficult and complicated;

operators need to be flexible with administration because they must use special adaption techniques while using some applications. The incorporation of the SDN into WSNs has been suggested as a solution to those problems. Also, a unique SD-related IoT paradigm has been formed as well (Figure 1). In the aforementioned paradigm, the two SDN layers (CP and DP) communicate via the Sensor-based OpenFlow (SOF) communication forms. Based on the provided table, the sensors send out data packets. The CPs are made up of one or more network controllers. By using SOF in this setup to execute the major flow table, users can achieve the completely programmable WSN. Both network control and network intelligence are conceivable (like routing and QoS control). The following are some of the features of SD-IoT:

(a) Multifunctional: Because they can support numerous plug-and-play programs, the sensor is no more dependent on the application's operating network. Remember that the network's logic functions are stored on the CP.

(b) Flexibility: The SD-IoT makes changing the entire method of network setup a simple operation. This assists network operators and device makers in avoiding incompatible local plans.

(c) Manageability: Only open APIs offered by the CP are required for network management solutions. This method can also be used to add new applications without having to change the main code. Using an AI-based network controller, network adaptability can be achieved, allowing for smart routing and QoS control [11].

The implemented SD-IoT paradigm, as shown in Figure 1, consists of three layers: the physical, control, and application layer.

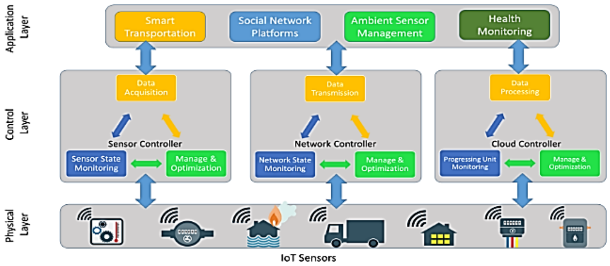


Figure 1: Software Defined-IoT's Structural Model

Deep Learning based Security System:

Deep learning is a subset of machine learning techniques focused on classification tasks and evolutionary algorithms [10]. There are three types of learning: supervised learning, semi-supervised and unsupervised. Deep-learning architectures incorporating deep learning models, fully connected networks, recurrent neural networks, and artificial neural networks were used in fields involving machine learning, artificial intelligence, computer vision, data analysis, realized, social media site filtering, computational linguistics, computational biology, drug design, information retrieval, and clear overview, among others. Knowledge acquisition and decentralized organizational infrastructure in biological systems influenced artificial neural networks (ANNs). ANNs vary from the human brain in several ways. In particular, neural networks are constant and symbolic, whereas most functioning entities' biological brains are dynamic and analog.

Deep learning gets its name from the fact that it employs many layers in the network. Early research demonstrated that a linear perceptron cannot be used as a universal classifier but that a network with a non-polynomial input layer and one unrestrained width hidden layer may [59]. Deep learning is a more recent variant involving many layers of bounded size, allowing for functional application and optimization while maintaining theoretical subjectivity under mild conditions. For the sake of performance, trainability, and intelligibility, deep learning structures are also allowed to be diverse and veer away widely from scientifically informed connectionist models, hence the "organized" portion [11].

The majority of new deep learning techniques focus on machine learning, especially convolutional neural networks (CNNs). They may also include propositional formulas or latent variables structured layer-wise in deep generative models like deep belief networks and deep Boltzmann machines. Each level of deep learning learns to turn the data it receives into a slightly more abstract and composite representation. The raw input in an image recognition program could be a matrix of pixels; the first representative layer could abstract the pixels and encode edges; the second layer could compose and encode edge arrangements; the third layer could encode a nose and eyes, and the fourth layer could recognize that the image contains a face. Importantly, a deep learning algorithm may figure out which features belong to which level on its own.

The term "deep learning" refers to the number of layers that the data is transformed through. Deep learning systems, in particular, have a significant credit assignment path (CAP) depth [5]. The CAP is the input-to-output transition chain. CAPs are used to define possible causal relationships between input and output. The depth of the CAPs in a feedforward neural network is equal to the network's depth plus the number of hidden layers plus one. The CAP depth in recurrent neural networks, where a signal can propagate through a layer multiple times, is theoretically unlimited. Although no generally agreed-upon depth level separates shallow and deep learning, most researchers agree that deep learning needs a CAP depth greater than 2. In the sense that it can imitate any function, CAP of depth two is a universal approximate [7].

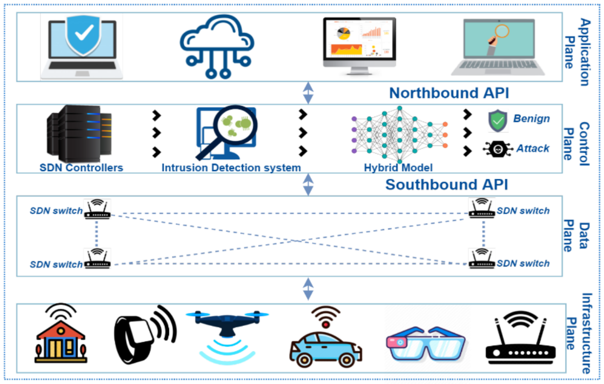


Figure 2: Deep Learning in SDN

IV. SIMULATION RESULT

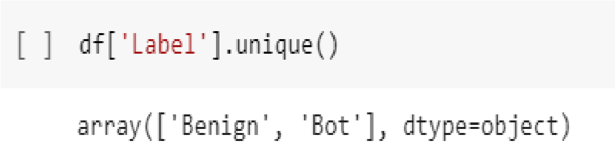
Step 1:- Data preprocessing

1.Load CIC-CSE 2018 dataset

2.Create pandas data frame

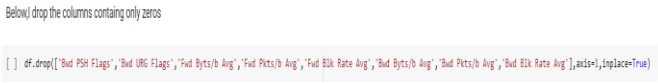
3.Describe data frame with (Count, mean, std , min, max), check data types of each columns

4.Print and check unique ness in data frame



```
[ ]  df['Label'].unique()

     array(['Benign', 'Bot'], dtype=object)
```

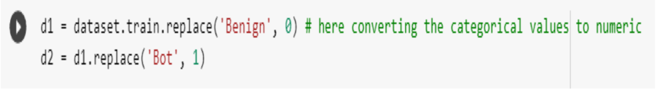
5.Check null values ,convert categorical and drop unnecessary columns



Below,I drop the columns containg only zeros

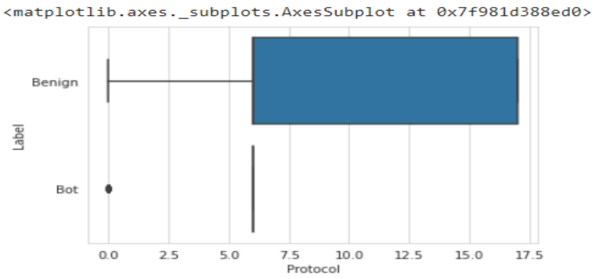
```
[ ]  df.drop(['Bwd PSH Flags','Bwd URG Flags','Fwd Byts/b Avg','Fwd Pkts/b Avg','Fwd Blk Rate Avg','Bwd Byts/b Avg','Bwd Pkts/b Avg','Bwd Blk Rate Avg'],axis=1,inplace=True)
```

6.Consider Label as Benign and Bot and do labeling string to numerical information

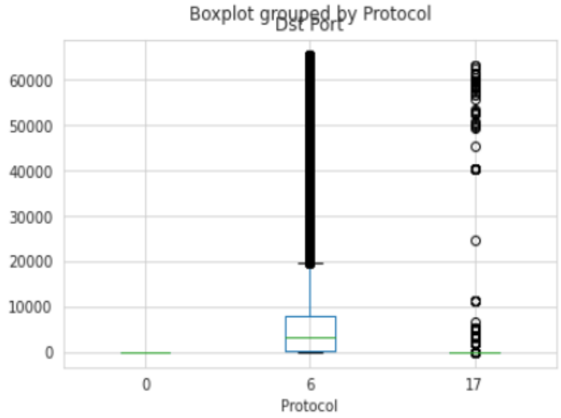


```
d1 = dataset.train.replace('Benign', 0) # here converting the categorical values to numeric
d2 = d1.replace('Bot', 1)
```

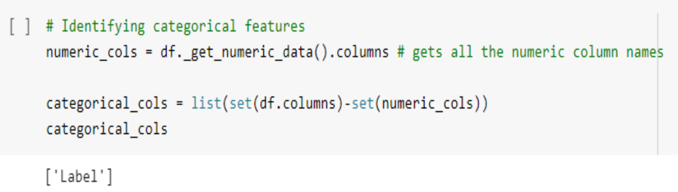
Step 2:- Perform Exploratory Data Analysis



```
<matplotlib.axes._subplots.AxesSubplot at 0x7f981d388ed0>
```

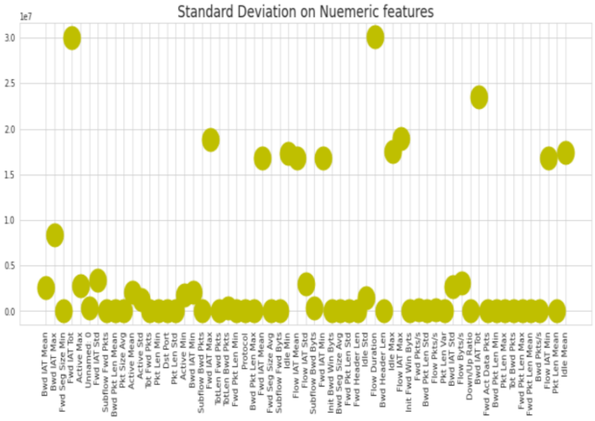


Identify Categorical features

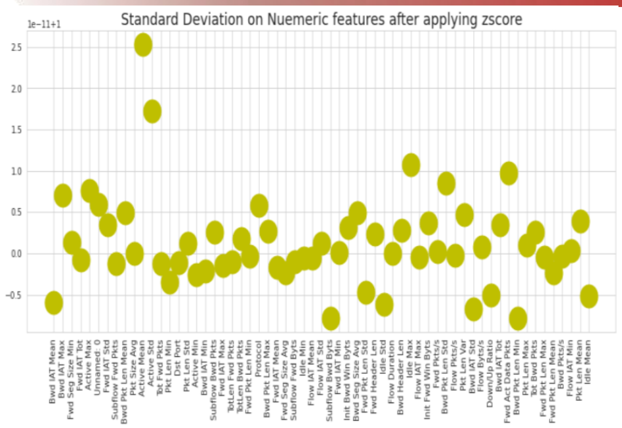


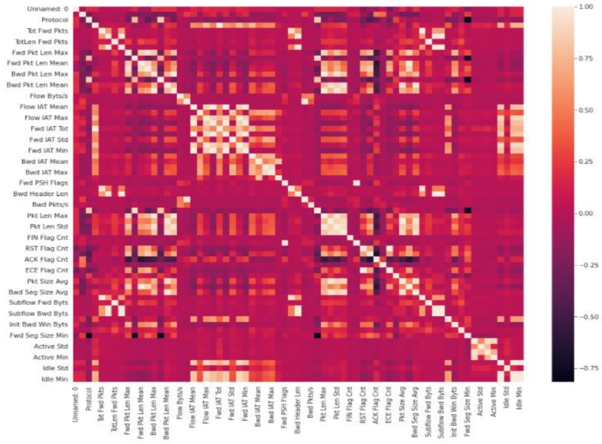
```
[ ] # Identifying categorical features
    numeric_cols = df._get_numeric_data().columns # gets all the numeric column names

    categorical_cols = list(set(df.columns)-set(numeric_cols))
    categorical_cols

    ['Label']
```

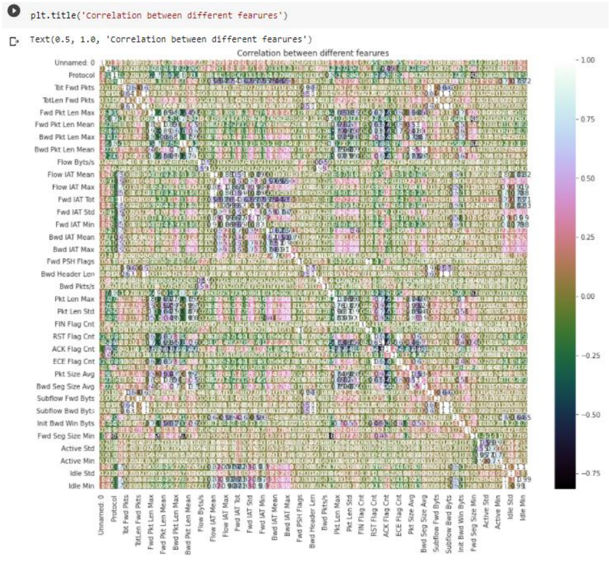
Numeric Features analysis



Journal of Validation Technology
ISSN: 1079-6630 E-ISSN: 2150-7090
(www.jvtnetwork.com)
Volume 29, Issue 1 – March 2023







```
plt.title('Correlation between different fearures')
```

```
Text(0.5, 1.0, 'Correlation between different fearures')
```

Step 6:- Results

Training and Testing Accuracy of Deep learning

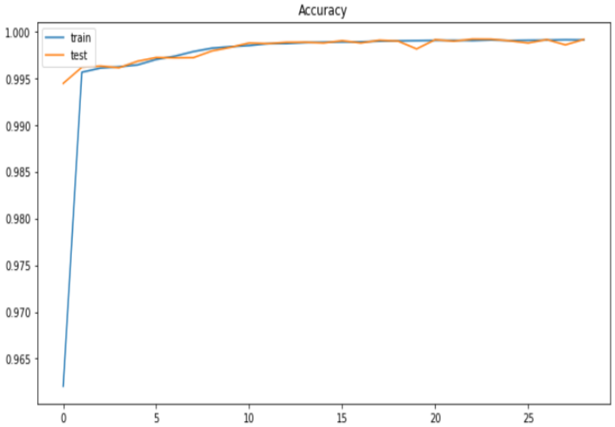


Figure 3: Graphical Represent of Acuracy

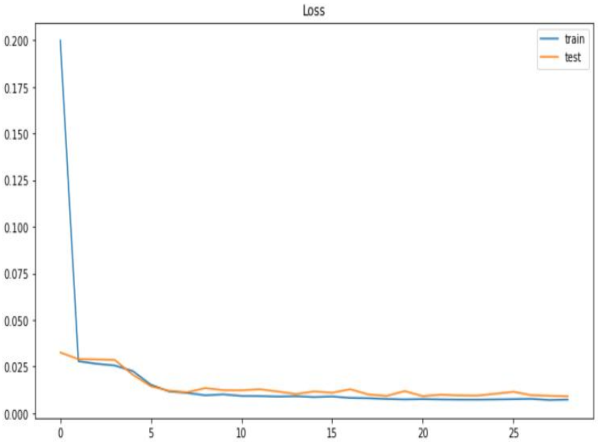


Figure 3: Graphical Represent of Loss

v. CONCLUSION

IoT frequently offers the data gathering, administration, and device and data protection services needed for application development. IoT things or gadgets interact and compute to improve the security and comfort of lives. IoT can be used for inventory automation, real-time item monitoring, and the administration of the information and state of things. The vast quantity of data that moves between the devices in the network necessitates the creation of a security structure that guarantees the integrity, secrecy, authentication, and permission of data. However, as the popularity of the app grows, so do security worries. SDN is a future trend for IoT security solutions.

REFERENCES

[1] Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[2] Jia, Y., Zhong, F., Alrawais, A., Gong, B., & Cheng, X. (2020). “Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks”. IEEE Internet of Things Journal, 7(10), 9552-9562.

[3] Jazaeri, S.S., Jabbehdari, S., Asghari, P., Javadi, H.H.S.: “Edge computing in SDN-IoT networks: a systematic review of issues, challenges and solutions”. Clust. Comput. (2021).

[4] Al-Amri, M.A. AlZain, J. Al-Amri, M. Baz, M. Masud, “A comprehensive study of privacy-preserving techniques in cloud computing environment”, Advanc. Sci. Technol. Eng. Sys. J. 5 (2) (2020) 419–424.

[5] Wang, W. Meng, W. Li, J. Li, W.-X. Liu, and Y. Xiang, “A fog-based privacy-preserving approach for distributed signature-based intrusion detection,” Journal of Parallel and Distributed Computing, vol. 122, pp. 26– 35, 2018.

[6] Dabbagh, B. Hamdaoui, M. Guizani, A. Rayes, “Software-defined networking security: pros and cons”, IEEE Communications Magazine 53 (6) (2015) 73–79.

[7] Benzekki, A. El Fergougui, A. Elbelrhiti Elalaoui, “Software-defined networking SDN: a survey”, Security and communication networks 9 (18) (2016) 5803–5833

[8] Furfaro, G. Malena, L. Molina, A. Parise, “A simulation model for the analysis of DDoS amplification attacks”, Conference on Modelling and Simulation, 2015, pp. 267–272

[9] Kumari, M. K. Khan, and M. Atiquzzaman, “User authentication schemes for wireless sensor networks: A review,” Ad Hoc Networks, vol. 27, no. November, pp. 159–194, 2015, doi: 10.1016/j.adhoc.2014.11.018.

[10] Chaudhary, S.; Johari, R.; Bhatia, R.; Gupta, K.; Bhatnagar, A. CRAIoT: Concept, review and application (s) of IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4.

[11] Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies. *IEEE Commun. Surv. Tutor.* 2020, *22*, 1372–1391.

[12] Adat, V.; Gupta, B.B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommun. Syst.* 2018, *67*, 423–441.

[13] Ahmed, M.I.; Kannan, G. Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications. *J. Inf. Knowl. Manag.* 2021, *20*, 2140004.