International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V68I11P218
Volume 68 Issue 11, 137-144, November 2020

Artificial Neural Network for the Internet of Things Security

Amit Sagu[#1], Nasib Singh Gill[#2], Preeti Gulia[#3]

Department of Computer Science & Applications
Maharshi Dayanand University
Rohtak, Haryana, India

[1]saguamit98@gmail.com,
[2]nasibsgill@gmail.com,
[3]preeti.gulia81@gmail.com

Abstract *– The Internet of Things (IoT) defines billions of devices that are tied to each other and sharing data via the internet or wireless network. IoT makes available the environment, including home, offices, and vehicles, smarter. With mounting the recognition of IoT, security challenges are growing too. IoT sensors assemble and share classified data, which means to be shielded from unlawful contact. For securing the IoT environment, numerous traditional approaches are being used. Some are lightweight encryption, create a separate connection for IoT devices, or defend against known spoofing identities. An innovative approach to secure IoT environment is employing Artificial Neural Network (ANN) [1], a machine learning model. ANN is a mimic of a biological neural network, which is an information processing model. It can be employed in the intrusion detection system between the IoT environment and outer network; it can also overpower traditional security methods.*

Keywords - *IoT, Machine Learning, Artificial Neural Network.*

I. Introduction

IoT is projected similarly to the internet, an interconnected network of the terminal, in IoT, it is related to small devices (things). These things have constrained characteristics in the context of their battery power, computation capability, or storage capacity. As IoT devices are low-priced and robust, its popularity is securing more interest day by day. The things can connect themselves with the internet and practice for sending and receiving data.

In IoT, there are primarily three sorts of things according to their functionality.

- A device which can collect data and send it
- A device which can receive data and act on it
- A device that can do both.

In agricultural farms, sensors are deployed to monitor temperature, and these sensors have the only job to collect the warmth and transmit it to the core. In another type is an actuator, a mechanical device with the ability to turn, move, push, or pull an object. This type of thing usually receives the lead in form of data and behaves correspondingly to it. The final type is more influential than the above two and having additional computation power. The advanced CCTV camera can turn in any direction and scan a learned pattern by analyzing the database and sending that data to pivot.

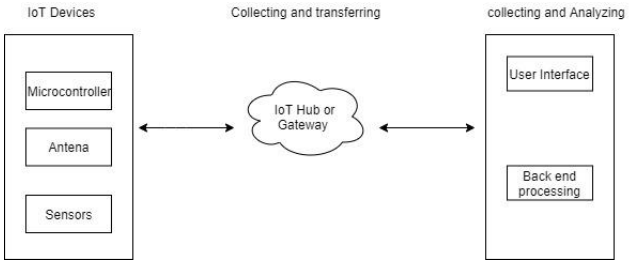

Fig. 1 IoT Architecture

A. IoT Application

IoT is supposed to be a revolutionary era and spreading its impact by taking the world to the next height. It is the idea of merging the real world and the virtual world by making human-device seamless communication. IoT can be utilized in daily life like the private sector, education, public sector, agriculture, security, and countless. Its flexibility marks it an appealing option for many businesses. Following are some applications of IoT:

Smart Homes are the most trending IoT application; according to an analysis by KRC Research, the smart appliance is the more apt device to utilize in the upcoming years.

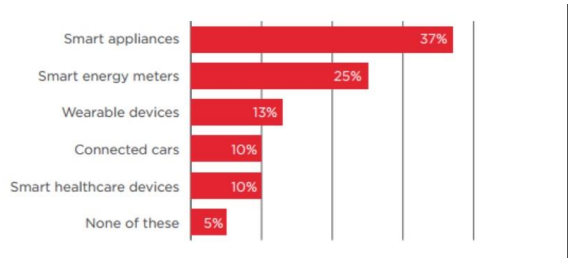

Fig. 2 (Source: GSMA Report)

A smart home's idea is to regulate house electronic device involving smart bulbs, water flow management, home security, and many more. Smart homes grant us to oversee all our home appliances from one corner. One can utilize a security camera under the IoT service to prevent thefts and robbery.

Smart City - Smart city is an influential use of IoT among the world's population. Supervision, transportation, energy management procedures, water supply, urban security, and environmental monitoring are instances of the internet of things applications for smart cities.

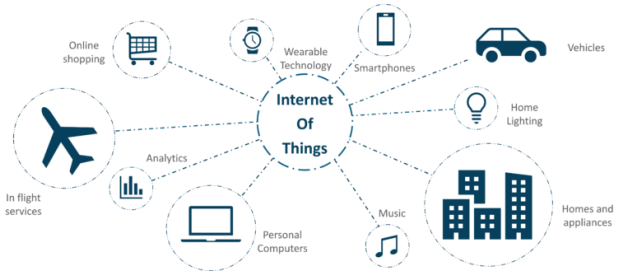

Fig. 3 IoT Applications (Source: Edureka. co/)

Healthcare - To assist stay healthy, IoT-connected devices are very effective. Fitness trackers facilitate tracking our everyday movements, for instance, napping patterns, heart rate, patterns of activity, measurements of workouts, calories consumed, etc. IoT makes it possible to put sensors on wear and supervise some signals. This sensor assembles data via skin interaction and transfers data to smartphones and remote analytical devices.

IoT in farming - Agriculturalists can use smart IoT farming products to enhance different processes, like deciding the finest time to yield crops, using soil fertilizer and spotting ground nutrients and humidity concentrations. An array of sensors can be mounted all through agriculture; sensors tied to animals can monitor livestock. For instance, a microchip is put on the ear to trace the animal, notifying its vaccine record, along with additional info.

B. IoT Security Challenges

As large numbers of IoT devices have made their existence into the world, implemented in uncontrolled, complex, and often hostile environments, securing IoT systems presents unique challenges. Follows are some top security challenges:

Secure Resource-Constrained Things – as we have seen earlier that IoT devices are constrained in the context of battery power, computation ability, and storage capacity. Security methods that depend on encryption are not decent for these limited ability devices, as they are not efficient in functioning complex operations swiftly sufficient to convey data securely in real-time.

Device Updates – Things often require updates, including security patches, software version revise, and spam request catalog update. Not every device support online update; they required to be physically retrieved to apply revises. Even when updates are presented, the user needs to be applying an action; they also must ensure that only legitimate updates are being applied.

IoT malware – As the IoT devices continue to increase, so the number of malware and ransomware used to exploit them. The malware attack could aim to control or immobilize device functionality and sneak consumer data simultaneously.

Untrustworthy Threat Recognition Approaches –Firms have various identifying data breaches, which include noticing common indicators, observing consumer movement, and other security procedures. But due to the increasing amount of IoT devices and the complexities of things, typical threat dedication techniques are less trustworthy and more of a challenge.

Inability to Predict Threat – if any model could predict any form of threat, it can be stopped outside the IoT environment. Detection systems need to be proactive to counter security breaches before they happen. We can build this type of detection system by applying machine learning algorithms.

C. IoT Common Attacks

IoT technology is changing the world and will continue to do so in the upcoming days. The hazards and risks stated below are certainly a challenge for enterprises in the IoT environment that intend to deliver an effective, secure, and wholesome facility that shields user information.

Several kinds of attacks have been around for quite a long time with the new scale and simplicity of attacks in the IoT environment. Millions of devices are possible target to conventional type attacks; some of these are the following:

A botnet is a web or network that merges numerous systems collectively to control the target's system and disseminate malware code remotely. Attackers can control botnets to sneak into classified information, acquiring banking details, and perform cyber-attacks such as DoS and phishing. They

can also use botnets to infect IoT devices, which are linked to many other devices such as cameras, desktops, and user interface devices. Mirai botnet is a very dangerous IoT security threat it ever can be.

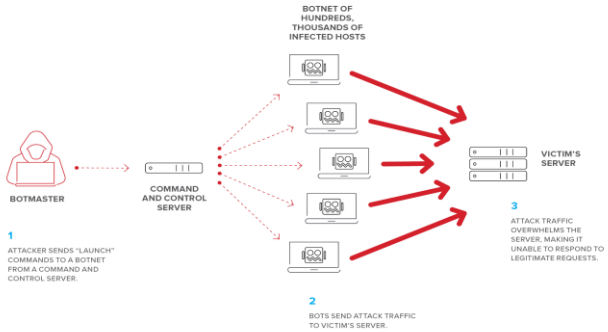

Fig. 4 Sigmoid Function

DoS (Denial of Service) – this type of attack purposefully attempts to cause a server or system stress by transmitting countless requests. It can also be employed to reduce speed or deactivate a service to damage any corporation's status. DoS does not typically attempt to sneak into data or breach the security, but the demise of any enterprise's character can still pay plenty of time and money.

Man-in-the-Middle Attack – This is the idea where any hacker or intruder is seeking to interfere and try to breach communications between two different individuals. It can be a serious hazard because, in this attack, the hacker surreptitiously intercepts and transfers messages between two individuals when they have confidence that they are conversing directly with each other. Since the intruder has the original message, they can trap the receiver.

Social Engineering – Attacker, can practice social engineering to trap people into offering their confidential data like passwords and bank details. On the other hand, an attacker may also employ social engineering to gain access to a system for establishing harmful or malicious code surreptitiously. Social engineering strikes are generally performed through phishing messages, where cybercriminals must create encouraging emails to influence users. Social engineering strikes are easier to perform in the case of an IoT environment.

Ransomware – This attack has grown to be one of the extremely infamous cyber-attack. During the attack, an attacker utilizes malware to encode information that may be necessary for enterprise functions. An attacker will decide to decode that information only when he is being paid a ransom. Ransomware can be used to attack into IoT environment or smart environment. For example, an attacker can attack a smart home network and warn the vendor to give a ransom.

II. Traditional Approaches for securing IoT

The popularity of IoT-connected devices has led to a rise in the demand for IoT development. Still, IoT development has its concerns and security challenges, which cannot be ignored. There are some traditional approaches used. Likewise, we will consider in what way they are appropriate.

Data Encryption – Among many approaches, encryption is identified as the basis of IoT security. Encryption is to transform the plain text into an unreadable form known as cipher. It is performed in conjunction with encryption algorithms and virtual keys. The key objective behind this to secure sensitive information from unauthorized access. The encrypted data can be decoded or decrypted with the key only, which is meant to have the receiver end. Without encryption, information is readable to anyone who has the intention to steal the data in the transition or stored in a server. These are some encryption methods:

- DES (Data Encryption Standard) [2]
- RSA (Rivest-Shamir-Adleman) [3]
- Triple- DES [4]
- AES (Advance Encryption System) [2]
- Blowfish [5]

To implement this approach on IoT devices may be troublesome due to their limited characteristics. Therefore, lightweight cryptography is a way for special kind of devices which have resource-constrained. For implanting the lightweight cryptography, some factors are to be considered like the size of primary memory (RAM), power consumption, processing delay, etc. lightweight cryptography may have complex computation over the devices causes lower the performance of IoT environment.

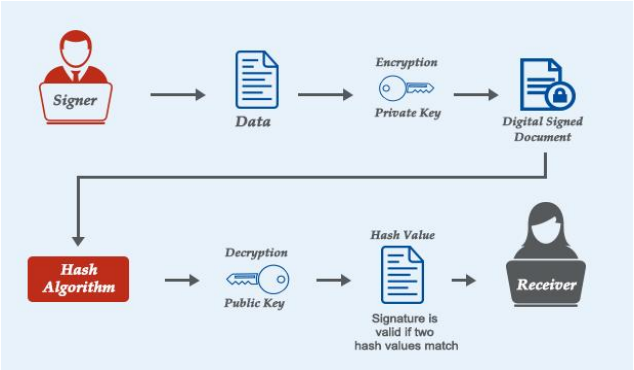

Fig. 5 Digital Signature (Source: comodosslstore.com)

Authentication – It means guaranteeing a safe and sound authentication of a single-user into several devices. In this area, applying two-factor authentication is extremely suggested, i.e., biometric and digital signature. A digital signature is a work on asymmetric cryptography in which two different keys exist. One is private, and another is the

public key. In the digital signature signer practice, use their private key to encrypt the message, and the recipient uses the sender's public key to decrypt that message. Client-server authentication is the simplest method in which the client and server share the authentication data before utilizing the service. The server has the catalog of users who can sign-in to the server and the directory of their authentication records, specifically password or the keyword's hash value. As a result, every IoT device requires a distinctive identity that can be authenticated once the device tries to link to a gateway. Along with unique ID, system administrators can trace every device all through its lifespan, convey securely with it, and halt it from executing destructive activities. If a device shows unanticipated behavior, the administrator can easily withdraw its privileges.

Securing IoT Network – IoT allows devices and daily-used things to be implanted with the internet to be remotely supervised and controlled from anyplace. It allows to remotely start cars, lock houses, and even control domestic appliances. It is extremely significant and necessary to develop methods to ensure the classified information is transmitted over the network. One of the key methods to safeguard IoT communications is using a Virtual Private Network (VPN). This Solution establishes a reliable private network over the internet, among linked devices and data centers. We can establish our own IoT private network to safely conduct and create relations with IoT devices safely and avert attacks that seek out to modify or snoop on IoT statistics. While also guaranteeing that only permitted devices can come to be a private element network.

Physical Security – IoT devices can be a precious element. These are the effortless target for an attacker as they are frequently tiny and can be stationed in isolated locations with no user in touch. The complicated connectivity of devices indicates that it might cause a domino effect throughout other devices if a single device is compromised. A basic role of confirming the security of IoT devices is to close needless ports. An additional aspect of the IoT is utilized of sensors that generate data. The integrity of the sensor being used depends on physical security. If a sensor can be influenced or merely defective, the created information may deliver biased and erroneous analytic outcomes. As a result, physical security is vital to involve in IoT security approaches.

III. Artificial Neural Network

ANN is a unique sort of machine learning algorithm which is developed by mimic the human brain. It is similar to how neurons in the human nervous system are intelligent to understand from past information. In the same way, ANN can learn from the information and deliver reactions in the form of predictions or classifications. Nonlinear statistical models demonstrate a complicated connection between the inputs and outputs to find a new pattern. An array of tasks such as pattern recognition, voice recognition, and classifications use these artificial neural networks.

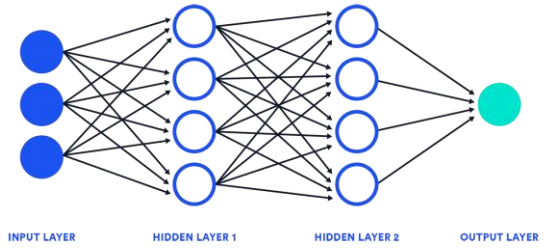

Fig. 6 Neural Network Architecture (Source: pngegg.com/en/png-pbana)

In ANN, there are three fundamental layers:

- Input Layer
- Hidden Layer
- Output Layer

The input layer is the primary layer of ANN, which accepts the input data in any written word, statistics, auditory files, picture pixels, etc. In the mid of the ANN, architecture is hidden layers. There can be only one hidden layer or multiple hidden layers. These layers act on different forms of mathematical computation on the received input information and distinguish the patterns and behavior of the output layer depending on the activity of hidden layers and the weights among the hidden layers.

ANN is efficient in learning, and it required to be trained. There are some learning approaches:

Supervised Learning – It includes a supervisor, which is help ANN to learn itself. The objective is to estimate the mapping so that when we have new input, we can predict the input variables. Few popular kinds of problems are constructed at the topmost of classification and regression.

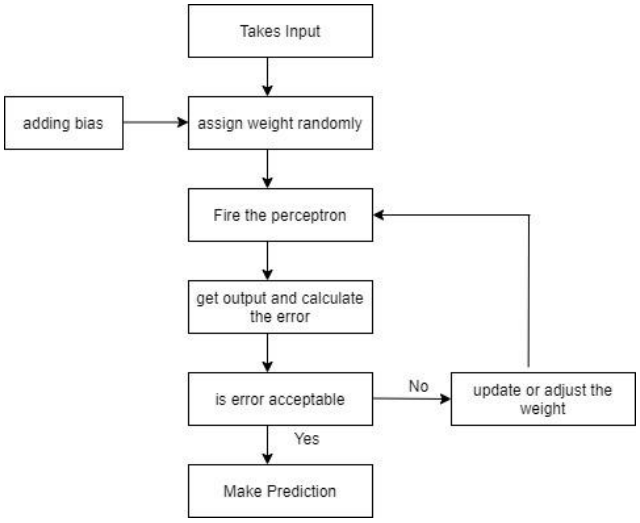

Fig. 7 Feed Forward Phase

Unsupervised Learning – Unsupervised learning is where we have only input variables and not having output variables. The objective of unsupervised learning is to model the fundamental building or dissemination in the data to know more about the data. Dissimilar to supervised learning, there are no precise answers, and there is no supervisor. Algorithms are left to their plans to find patterns in the data.

In ANN algorithms, we provide independent variables that mean input data and dependent data, which means to output data. At starting, the ANN makes several arbitrary predictions. These predictions are contrasted with the actual or corrected output, and the error (the difference between the propagated values and the actual values) is computed. The function that discovers the contrast between the actual value and the predicted values is called the cost function. Here the meaning of cost is an error. The goal is to reduce error to the actual values. Training an ANN refers to lessening the cost function.

ANN performs in two phases, i.e., Feed Forward and Back Propagation phase.

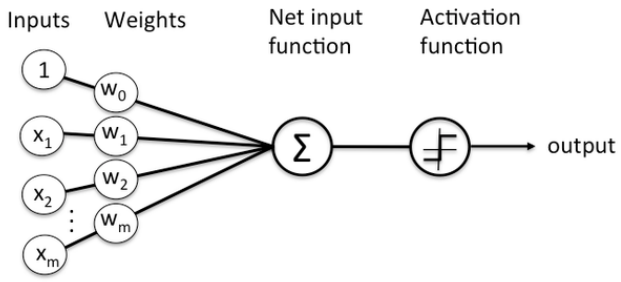

Fig. 8 Feed Forward Phase

Feed Forward – In this phase of ANN, predictions are prepared based on the input nodes' beliefs and weights. The weights of ANN are the factors that we try to modify to predict actual output values appropriately. We have one weight corresponding to each input feature.

$$X1.W1 + X2.W2 + X3.W3 + \ldots\ldots X_n.W_n \qquad (1)$$

The nodes of the input layer relate to the output layer through some weight. In the output layer, the input values are multiplied with their weights, respectively, and make the sum (1). Also, the bias is added to the sum result. The bias is required to get a robust ANN. The resulting values are passed to the activation function, restricting the values in a specific set of values. For instance, in fig 1 (2), the sigmoid function always gives the values between 0 and 1. This type of function is known as the activation function.

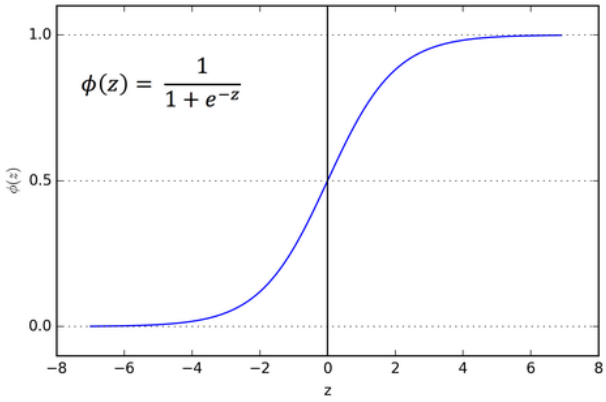

Fig. 9 Sigmoid Function

The sigmoid function gives 0.5 when we take input 0, and it returns a value near to 1 if the input is a large positive number. Intake negative input, then the sigmoid function returns output close to zero.

$$S(x) = \frac{1}{1+e^{-x}} = \frac{e^x}{e^x+1}. \qquad (2)$$

Back Propagation – Before this Phase, ANN makes a random prediction far from correct values. But this is the initial stage after we compare the predicting result with the actual result to update the weights according to it, and prediction can come closer to actual values. This is the backpropagation phase; in this phase, we train our ANN.

The first step in the backpropagation phase is calculating the cost function, which is the difference between actual values and predicted values. The mean squared error (MSE) cost

function is used to cost function. But our ultimate objective is to minimize the cost or minimize the error. We reduce the error by adjusting the weights and bias as we cannot change our input nodes. To find the minimum cost function gradient descent algorithm can be used.

A. ANN for IoT Security

Machine learning has witnessed considerable growth across a large scale of applications in the modern years, and it will be essential in securing the IoT environment. Addressing IoT security in a smart environment with the security of traditional and generic computing devices is not feasible.

There are too many challenges, like overseeing countless devices, having a computer or two, a smart device, and many more. Each requires the installation and maintenance to shield them against threats. Think of requiring managing updates, credentials, and settings for lots of linked appliances single-handedly with no endorsement of an IT security unit.

Here machine learning comes into the picture. In many organizations, it is supplementing human effort and making up for the lack of human resources. Machine learning is particularly skilled at learning and determining patterns, mainly when supplied with gigantic amounts of information. There is always lots of data present in the IoT environment and quite a few real use cases where machine learning can enhance IoT security.

B. Network-based Solution

Considering each device's security, network-based solutions can guard IoT devices by establishing an armor across the IoT network. It involves identifying and registering each IoT thing authorized to log in a group to avert invaders from stepping into the IoT environment. However, IoT appliances must also have gain access to and be retrieved from third parties like cloud servers and mobile applications interface. The machine learning algorithm can examine arriving and outgoing IoT device traffic flow to generate a pattern that defines IoT devices' usual behavior. Exposing dangers will help uncover traffic and decide that it does not come inside the usually formed behavior. Warnings can be forwarded to the device authorizer to inform them about possible threats and irregular device behavior.

C. ANN Compared with Other Classifier

ANN classifies the results by taking input variables via a chain of neuron layers known as hidden layers, which execute complicated transformations on the given information. It is incredibly efficient for high-level dimensionality tasks or along with multifaceted relations among variables. For instance, ANN can be applied to classify and label pictures, audio, and video, do sentiment evaluation on wording, and categorize security threats. But ANN is supposedly complex, tricky to employ, needing delicate adjusting, and computationally demanding. Unless we are deep learning specialists, it will typically derive additional value apart from the classification algorithm.

While working on machine learning projects, we can probably experiment with other classification algorithms or classifiers if we are not restricted to use ANN. We can utilize open-source Python libraries such as scikit-learn, which offers fashioned implementations of trendy classifier and is comfortable to get began with. If we need to use ANN classification, we will need to use deep learning frameworks such as TensorFlow (fig. 8), Keras, and PyTorch. These frameworks are extremely effective, favoring both neural networks and other classifiers like decision trees and random forest trees.

```
import tensorflow as tf

#model parameter

w=tf.Variable(.3,tf.float32)
b=tf.Variable(-.3,tf.float32)

#model input and output
x=tf.constant([1,2,3,4],tf.float32)
y=tf.constant([0,-1,-2,-3],tf.float32)

model=w*x+b

#loss
error=model-y
square=tf.square(error)
loss=tf.reduce_sum(square)

#optimizer
optimizer=tf.train.GradientDescentOptimizer(0.01)
train=optimizer.minimize(loss)
```

Fig. 10.1 Implementing ANN using TensorFlow (screenshot)

IV. Artificial Neural Network vs. Traditional Approaches

Lightweight Cryptography – in this approach, we encrypt the transmitting information in a complex cipher that is nearly impossible to decipher, not including a virtual key. But implementation is a great challenge. As we know, IoT devices are resource-constrained, have low computation capability, and have low power battery. Lightweight cryptography may be hard on IoT hardware since it may require larger RAM or ROM size. In contrast, the machine learning concept may be helpful since it does not put stress on devices. ANN works between the IoT environment and outer network and examines the incoming traffic, whether malicious or benign. If there are any network patter other than not define already, it will alarm the user for a security threat.

Authentication means that we have to list all the registered or authorized users who can gain access to the IoT environment facility. Other than the registered user will not be authorized to access the network. This methodology is

quite excellent, but not nowadays. Attack named man-in-middle can sidestep this security fence certainly. Machine learning techniques can confront this challenge by utilizing complex algorithms. If we apply the machine learning concept, it will recognize the registered user and additional parameters, such as the sender's location, the packet size of the received message, time interval among packets arrival, and many more. These parameters are known as features that help the machine learning algorithm decide whether incoming network traffic normal for a security attack.

```
with tf.Session() as sess:
    sess.run(tf.global_variables_initializer())
    # sess.run({x:[1,2,3,4],y:[0,-1,-2,-3,-4]})
    # print(f"input x is {sess.run(x)}")
    # print(f"output y is {sess.run(y)}")
    # print(f"model is {sess.run(model)}")
    # print(f"error  is {sess.run(error)}")
    # print(f"square error  is {sess.run(square)}")
    for i in range(5000):
        sess.run(train)
    print(f"sum of error  is which is loss {sess.run(loss)}")

    print(sess.run([w,b]))
    # print(sess.run(b))
    # print(sess.run(loss))
```

Fig. 10.2 Implementing ANN using TensorFlow (screenshot)

Securing Network – instead of securing the IoT device, we can secure our network to transmit the information. We do this by creating a virtual private network. It is like a reserved tunnel for specific users, and not another user can use it. VPN a very good security method, but it is not free to use. Users must pay for the VPN service always. This method is suitable for securing the IoT environment in any enterprise but not acceptable for a normal user with a limited number of resources in his environment. So here, machine learning can be helpful again. It may be required to update the classifier, which is not a big deal.

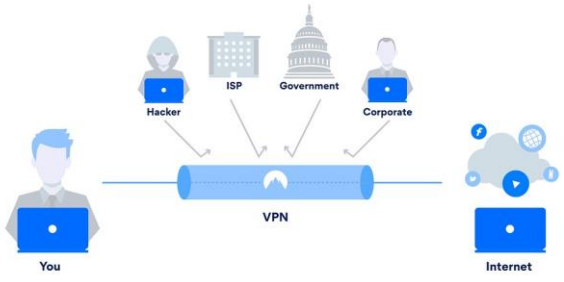

Fig. 11 Virtual Private Network Architecture

Physical Security – this is a very traditional or simple method to secure IoT devices. We physically secure devices Several datasets like DARPA, KDD 99, and LBNL (the academics are using Lawrence Berkeley National like CCTV cameras or sensors by fencing them around or using another method in this method. But this is the most vulnerable method in IoT security.
There are two types of physical vulnerability; these are:

- The non-invasive attack involves the hacker being close sufficient to exploit the chipset and track electrical signals. This allows the hacker to alter the conduct of the device or collect classified data.
- An invasive attack requires the chipset shell to be exploited, meaning that the device can be physically controlled.

Side-channel analysis is a non-invasive threat in which a hacker is analyzing power signature or Electric Magnetic pluses emitting from an IC (Integrated Circuit) to exploit classified data.
Tamper attack is an invasive attack where an attacker physically manipulates the IC intending to collect classified data in the wires using microcomputer surveys. An attacker might even attempt to change the IC conduct by overwriting the form of the circuit.

V. Future Approach

In our future approach, we will implement the testbed by using various attack datasets most ordinary is DDOS attack. Comparing the ANN with other machine learning classifiers to see how it performs when it encounters threat traffic flow. It might be possible that other than ANN classifier has more accuracy in some cases. While testing, we will ensure using all sorts of features to obtain convincing conclusions like packet length, packet interval time, etc.

Sr.	Features
1	Packet Length
2	Packet Interval Time
3	Source Port
4	Destination Entropy
5	TCP Flags
6	Source Address
7	Mean of IP length
8	Source Port Entropy

Table. 1 Features

Feature selection is an essential phase in the pattern recognition procedure and specifies the smallest achievable group of variables adept at effectively defining a group of classes.

Laboratory and ICSI to evaluate the proposed intrusion detection system's performance.

Though, these such datasets are outdated and erratic to use up. In our approach, we would use the datasets CIC-DoS, CICIDS2017, and CSE-CIC-IDS2018 and customized datasets as they consist of new threats.

VI. Conclusion

This paper has presented IoT security challenges and delivers the potential Solution to address those threats. Numerous traditional approaches such as lightweight cryptography, securing network, physical security, and authentication of devices were considered and perceived in what way they enact and their significance in IoT security. Following, comparing approaches with machine learning algorithms, it is convincing that ANN can be an efficient approach to confront IoT security attacks. The traditional approach may have a troublesome implementation on resource-constrained IoT hardware. We have compared ANN with other machine learning classifier models to evaluate their performance and know why ANN is most appropriate for security reasons. The further paper intends to spotlight the architecture of the neural network of both phases: forward and backward phase along with sigmoid activation function and discussed future work reference.

References

[1] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial, IEEE, (2019) 3039 - 3071.

[2] D. sukhija, A Review Paper on AES and DES Cryptographic, International Journal of Electronics and Computer Science Engineering, pp. 354-359.

[3] M. F. Shireen Nisha, RSA Public Key Cryptography Algorithm – A Review, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 6 (07) 2017.

[4] M. Karthik, Data Encryption and Decryption by Using Triple-DES and Performance Analysis of Crypto System, International Journal of Scientific Engineering and Research (IJSER), 2014.

[5] A. Alabaichi, F. Ahmad and R. Mahmod, Security analysis of blowfish algorithm, 2013 Second International Conference on Informatics & Applications (ICIA), IEEE, 2013.

[6] K. A. Taher, B. M. Y. Jisan and M. M. Rahman, Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection, International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), IEEE, 2019.

[7] N. Chauhan, A. K. Bhatt, R. K. Dwivedi, and R. Belwal, Accuracy Testing of Data Classification using Tensor Flow a Python Framework in ANN Designing, International Conference on System Modeling & Advancement in Research Trends (SMART) 2018.

[8] X. Sui, Q. Wu, J. Liu, Q. Chen and G. Gu, A Review of Optical Neural Networks, IEEE Access, 8 (2020) 70773 – 70783.

[9] S. Lin, J. Zeng, and X. Zhang, Constructive Neural Network Learning, IEEE Transactions on Cybernetics, vol. 49(1) (2019) 221 – 232.

[10] A. Mukherjee, D. K. Jain, P. Goswami, Q. Xin, L. Yang and J. J. P. C. Rodrigues, Back Propagation Neural Network-Based Cluster Head Identification in MIMO Sensor Networks for Intelligent Transportation Systems, IEEE Access, 8 (2020) 28524 - 28532.

[11] A. Jaiswal, A. S. Manjunatha, B. Madhu and M. P. Chidananda. Predicting unlabeled traffic for intrusion detection using semi-supervised machine learning : International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 2017.

[12] N. Shi, X. Yuan, J. Hernandez, K. Roy, and A. Esterline, Self-Learning Semi-Supervised Machine Learning for Network Intrusion Detection, International Conference on Computational Science and Computational Intelligence (CSCI), 2018.

[13] P. P. S. M. I. a. H. H. Chaoyun Zhang, Deep Learning in Mobile and Wireless Networking: A Survey, IEEE, 2019.