Webology (ISSN: 1735-188X)
Volume 18, Number 4, 2021

An Energy Model For The Iot: Secure Networking Perspective

Namita Jain[1] , Dr. Manju Mandot[2]

[1]Research Scholar (CS) , Janardan Rai Nagar Rajasthan Vidyapeeth University , Udaipur.

[2]Professor, Department of Computer Science, Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur.

ABSTRACT

General uses of the Internet of Things (IoT) include health care systems, energy management, monitoring the environment, home automation, and business automation. The Internet of Things is thought of as a service activation technology, but it also makes security and privacy much better. This thesis is about how to make a data source security agreement that verifies identity and protects privacy. The goal of the method is to make it take more energy to authenticate devices in security approaches. In the elliptic curve method that was suggested, cryptography is used to increase security with smaller key sizes and protocol changes for a more efficient authentication process. Other neural back propagation ML models helped with this work to find network attacks, improve networks, cut down on network overhead, and lengthen the life of networks. Using the lightweight authentication protocol, the proposed system creates a secure network that limits the damage that an attack on the IoT environment can do. Simulation performance has been shown with the help of MATLAB. This simulation compares how well a system works during an attack and after the attack has been stopped.

INTRODCUTION

The Internet of Things (IoT) is a modern computing model that refers to interconnected material devices or IoT devices containing sensors, actuators, and networking so that these IoT devices can link, communicate and share data. With rise in number of IoT devices, several security concerns have been found, especially in sharing of sensitive data. Authentication is one of these reliability concerns. In the IoT world, authentication is a major challenge due to complexity of protocols, devices, or topologies. IoT systems interacting with each other need to be trustworthy in order to prevent various forms of security negligence attacks. Authentication is also the cornerstone of access management and transparency. The Internet of Things (IoT) consists of knots with minimal resources, which, regardless of time or place, are widely dispersed in the IoT environment. IoT is now used for a wide range of purposes, including hospitals, intelligent homes, intelligent manufacturing, and intelligent cities. Furthermore, a hypertext net age can be used between

different handheld terminals, but most (if not all) of our applications, thanks to the advent and marketing of the fifth-generation (5G) cellular network, which is also possible. Link information between objects or exchange information. By 2022, it is expect that 43 billion devices will be related to IoT around globe, and the numbers of such systems are probable to amplify exponentially with marketing of 5 G networks. The massive Things network internet can deal with approximately 1 million items per square kilometer, depending on the 5 G Vision Specifications from the Radio Communications Department of International Telecommunication Union (ITU-R).

ARCHITECTURE OF IOT

The researchers proposed various types of IoT architectures, such as 3-tier, 4-tier, and 5-tier architectures. Though, these different architects identify 3 functions of the Internet of Things, such as vision, transmission or processing [9].

Perception Layer- The Internet of Things view layer is the layer that defines multiple Internet of Things objects, such as sensors, RFID, actuators, and mobile phones. The major functions of this layer are the acquisition, collection and processing of data from sensory procedure such as RFID, temperature or wetness sensors, usable materials or actuators that act as such. heaters and fans [10]. This level is dependable for converting information composed from the cells into a digital signal to be transmitted to upper network layer.

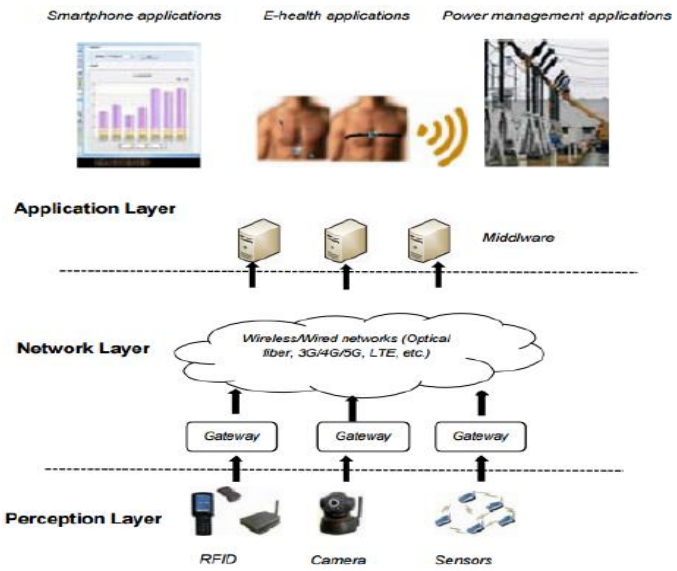

Figure 1: 3-layered Architecture of Internet of Things

Types of Internet of Things The "things" of Internet of Things can be divided into the follow categories [11]:

Tagging things: Items such as RFID are classified as tagging items.

Sensing things: Objects such as sensors in wireless sensor networks are classified as perceptual objects.

Shrink things Items such as nanomaterials, nanotechnology and nanoprocessors can be classified as shrinking items.

Sensing is a category of equipment used in follow division.

DEVELOPMENT OF WSN TOWARDS IOT

The Internet of Things consists of a variety of devices, or IP addresses assigned to these devices connect to a global network via the Internet. different IoT applications, such as healthcare and agricultural function, can be deployed based on requirement that wireless networks (WSNs) connect to real-time devices. This IP forwarding node transfers information to central node, which does all storage or organizes large sensor data produce.

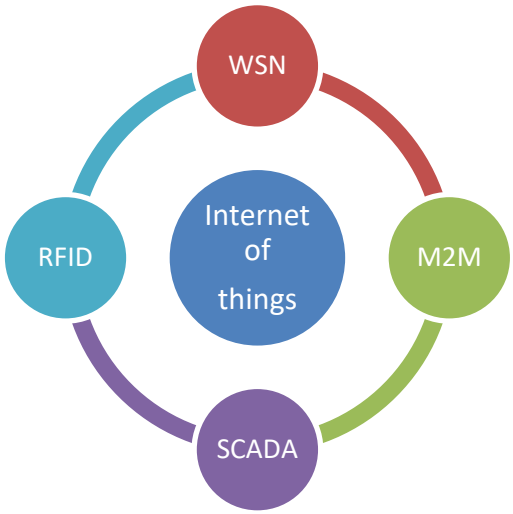

Figure 2: Role of WSN in IoT

It is accomplished through a dedicated gateway, which is also answerable for flow of data among devices in the IoT world. though, when we connect WSNs to the IoT, we will face a variety of challenges, including issues of security, application quality and application management .

OBJECTIVES

The follow objectives have been set to achieve planned work in problem definition:

1. To assess the current state of the IoT and to look at the causes for the relatively low security standards.
2. Providing solutions to the problems troubling the IoT.
3. To design the secure lightweight authentication protocol to mitigate the effect of the attack in the IoT network.

4. To perform a back propagation neural network for supervised learning to optimize the IoT network to reduce overhead consumption.
5. To find the most recent and relevant solutions to solving the problems of securing data communication from highly constrained devices to the internet
6. To design the secure lightweight authentication protocol to mitigate the effect of the attack in the IoT network.
7. To implement the man-in-the-middle attack for the efficient analysis of system.

ARCHITECTURE OF PROPOSED MODEL

The goal of the plan is to bring to light the fact that using current security methods to authenticate devices takes a lot more time and energy than is currently done. The cryptography strategy could be used in the proposed variations of the elliptic curve to provide more security with smaller key sizes and a more efficient authentication process by changing the protocol. This can be done by making the same number of key sizes more secure. Also, the other solutions can be contributed to using machine learning models where it can be used to detect the attacks and enabling IoT security systems to make adjustments in changing environments as per requirements. The purpose of this protocol is to use the public key to be used in next step of communication connecting devices to achieve device verification and secure key placement. In addition, there are other security objectives that can be achieved, such as counteracting layer attacks (such as simulation attacks), and attack recovery (while preserving integrity and capability).

The proposed protocols can likely be organized in below scenario of wireless body area complex and that can incorporate in IoT. Figure 3 shows a proposed Deployment Scenario

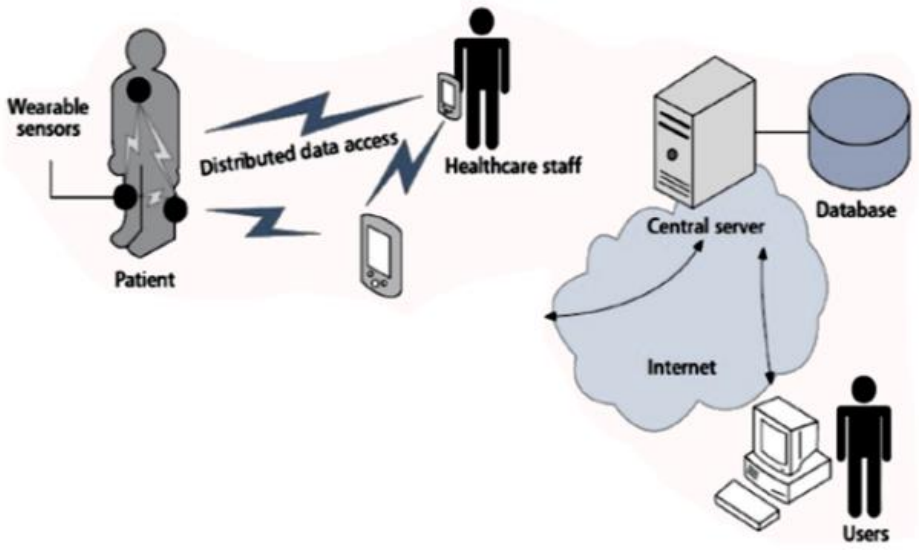

Figure 3: The proposed Deployment Scenario

The patient's sensor will commune with the medical staff through a gateway, as shown in Figure 3. When the patient's equipment issues an emergency notification to the medical staff. Will immediately communicate to him details of the medication. However, if attacker is able to use patient's equipment, he or she can send a false alarm to the staff, as a result, giving the wrong medicine to the patient and this endangers the patient. Therefore, prior to patient contact, a verification mechanism should be added between the patient device or gate. Likewise, employee equipment.

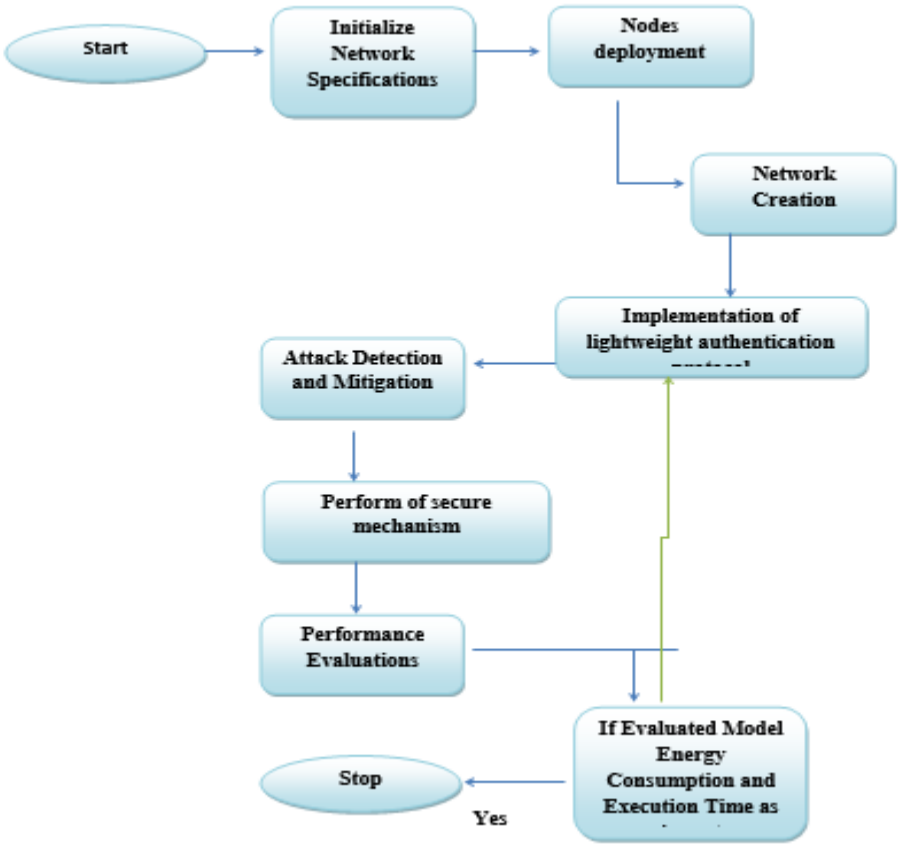

Figure 4 Proposed Flow Diagram

Algorithm

3.1 Device Registration Phase

1: D → G : Sends Id or EP uk (pwd), Password pwd encrypted with Elliptic Curve Diffie-Hellman symmetric key Dk

2: G : Decrypts message to find password pwd or Computes the shared secret value SK = H (Id ‖ V), P = SK ⊕ pwd 3: G → D : Sends P

Device Authentication Phase

Algorithm

1: D : Generates random number Nd, Computes SK′ = P ⊕ pwd

2: D → G : Message M1 = Id, ESK′(Nd)

3: G : Computes SK = h(Id‖v), N ′ d by decrypting ESK′(Nd) with SK, produce random number Ng

4: G → D : Message M2 = ESK(N ′ d ‖Ng)

5: D : recovers N ′ d , N ′ g by decrypting M2 using SK′ , verifies Nd = N ′ g and computes session key K = Nd ⊕ N ′ g

6: D → G : Message M3 = ESK′(N ′ g)

7: G : recovers N ′ g by decrypting M3 using SK and verifies Ng = N ′ g , Computes session key K = N ′ d ⊕ Ng

EXPERIMENT RESULT

Figure 5 shows simulation based on a network of 30 nodes. Throughout the entire network used as an administrator, the monitors malicious activity in network. The simulation was done using MATLAB software. This section discusses the use of symmetric core protocols and ECC encryption for device authentication and machine learning -based technologies to detect and protect malicious activity. Whatever the worthy application of the WSN, it is most vulnerable to attacks by hackers, such as human-to-human attacks (MITM).In the event of an MITM attack, an unsolicited third party will log in as a legitimate user in a short period of time. The attacker or attacker behaves like a proxy user and manipulates the data according to their needs. In the ancient literature, MITM was abbreviated in various ways, such as MIM. MITM Attack MITM is a malicious attack that secretly listens to the conversations of two legitimate users of the attacker. When necessary, the attacker pretends to be a legitimate user and attacks data or information for manipulation. Often, during a MITM attack there will be new discussions or transfers. Without reliable security, two legitimate users will not know the authenticity of the data .This work mainly examines the MITM Intrusion Detection System (MITM-IDS) based neural network study. The whole process tries to create attack-resistant MITM-IDS to ensure non-attack communication when unclean points are detected.

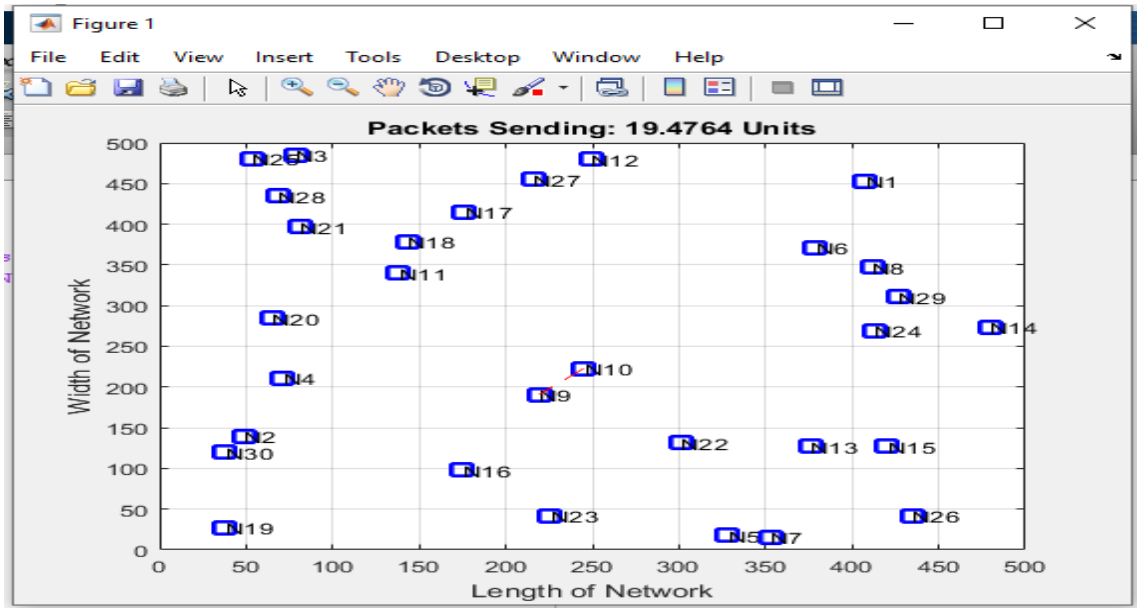

Figure 5 Initialization network

Data from the public node is sent to the source routing node in the region to execute the route request, and the source node adds the information of the selected route to the source routing header in it. In a data packet, In addition, in the data transmission process, the transmission point between the intermediary points follows the relay path and progress according to the source path information in the packet head, and no connection to the source routing node, which can reduce the energy consumption of the system.

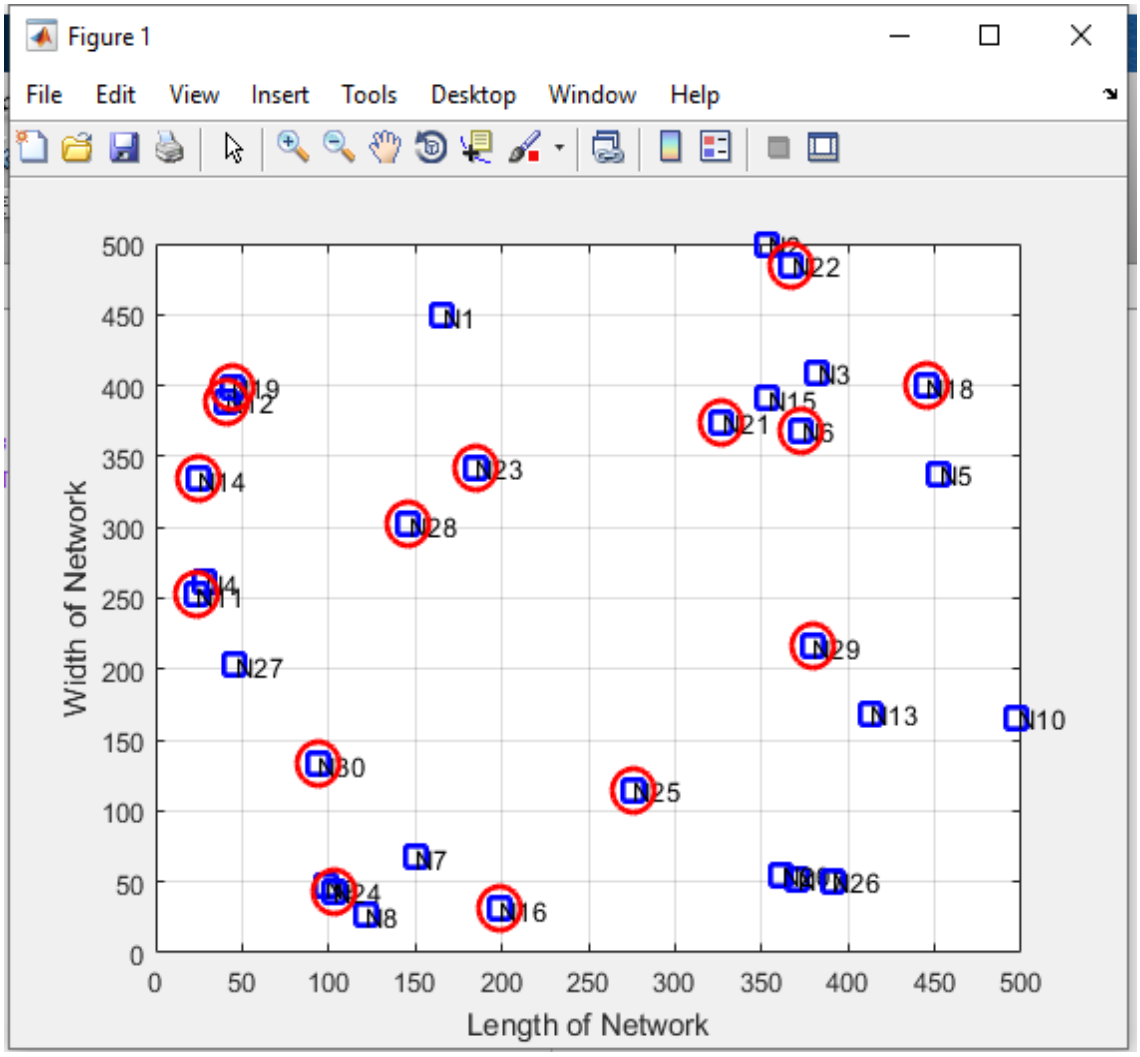

Figure 6 Device Registration

Figure 7 shows the energy consumption provided for the system.As the coverage area increases, the energy consumption also increases, mainly due to the distance between the member and the single CH. The energy balance is determined by the energy consumption of the equipment and the transmission power of the wireless sensor network. In the figure, the y axis shows the energy consumption, and the x axis shows the number of nodes.

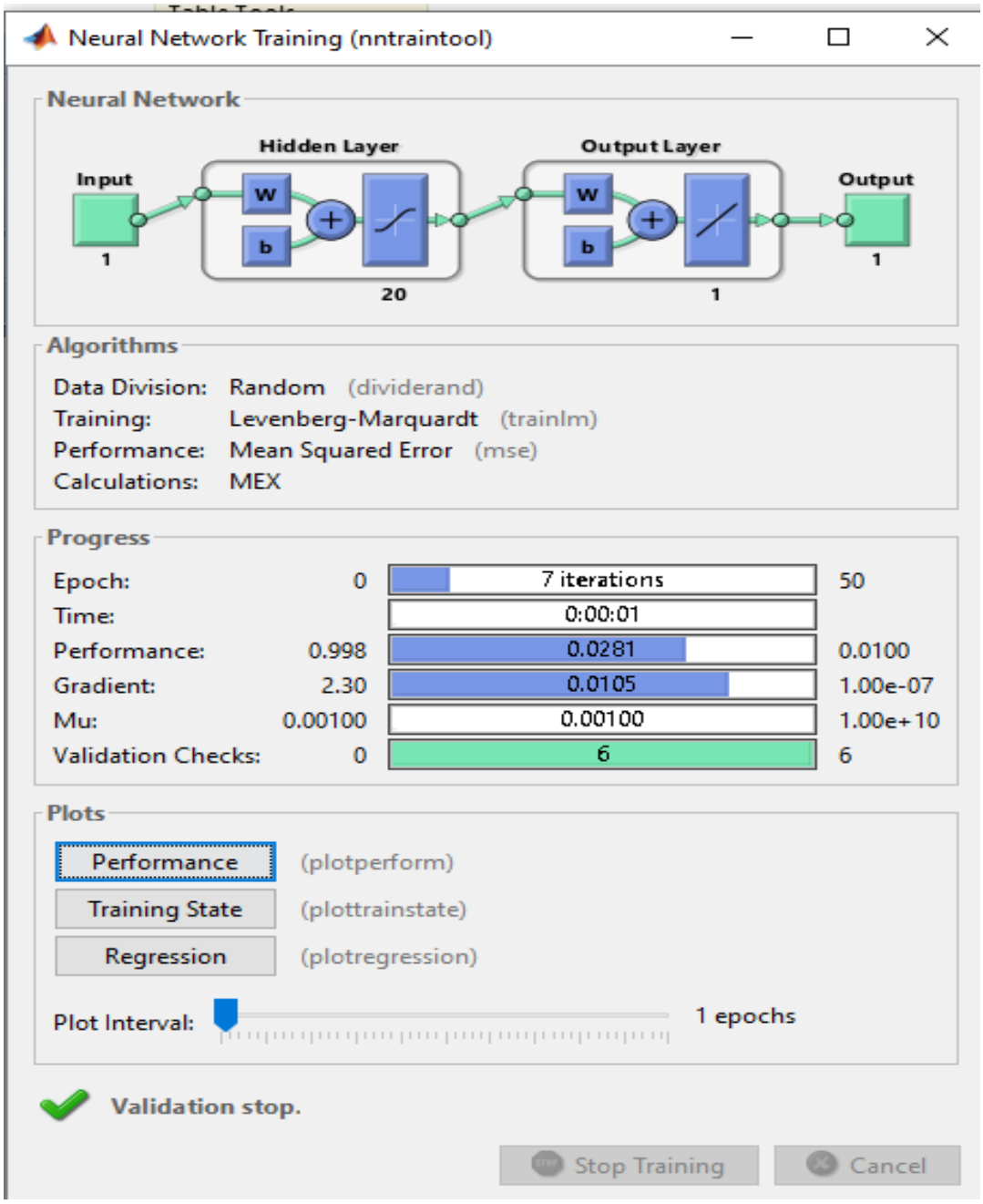

Figure 7 Neural Network Training

CONCLUSION

In this Paper , focus mainly on the challenges of the Internet. Then, we solved the validation problem in the perception layer of the Internet of Things. We have noticed that existing verification methods are still under attack, and some of them will overtake the head of the device. We propose a validation mechanism based on a symmetric base agreement, which uses ECC at the registration process and performs a symmetric base configuration at the end of the protocol validation process. Then, use this key between devices to perform data collection tasks.

We can see that the strengthening of cooperation has been achieved. Based on the analysis of the performance, because the key to using the cryptography ECC is small, compared to the existing method, this method is also light and easy to use. But in the security survey, we found that the protocol may be vulnerable to attacks by people in the middle. Therefore, at the end of the authentication process of the protocol, an asymmetric key agreement-based authentication mechanism is implemented, which uses an elliptic curve-enabled encryption scheme during the registration partition and assigns a symmetric key. This key can be used for data collection tasks between devices. We can see that the verification of both parties can be performed by this method. Based on the analysis of the performance, the proposed method is only light compared to the existing methods, but we can make exchanges in terms of safety and lightness.

REFERENCES

1. Data Provenance for IoT with Light Weight Authentication and Privacy Preservation Muhammad Naveed Aman, Mohammed Haroon Basheer, Student Member, IEEE Biplab Sikdar, Senior Member, IEEE 2327-4662 (c) 2019 IEEE.
2. M. H. Rehmani and A.-S. K. Pathan, Emerging Communication Technologies Based on Wireless SensorNetworks: Current Research and Future Applications. CRC Press, 2016.
3. D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.
4. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393–422, 2002.
5. Sazonov and M. R. Neuman, Wearable Sensors: Fundamentals, implementation and applications. Elsevier, 2014.
6. Blilat, A. Bouayad, N. el houda CHAOUI, and M. Ghazi, "Wireless sensor network: Security challenges," in Network Security and Systems (JNS2), 2012 National Days of. IEEE, 2012, pp. 68–72.
7. K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence andSecurity (CIS), 2013 9th International Conference on. IEEE, 2013, pp. 663–667.
8. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
9. M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7–10, 2008.
10. M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: State of the art," in Robots and Sensor Clouds. Springer, 2016, pp. 55–75.
11. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th InternationalConference on. IEEE, 2012, pp. 257–260.
12. X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012, pp. 1282–1285.

13. Y. R. Shi and T. Hou, “Internet of things key technologies and architectures research in information processing,” in Applied Mechanics and Materials, vol. 347. Trans Tech Publ, 2013, pp. 2511–2515.
14. Hakjun Leea, Dongwoo Kanga, Jihyeon Ryub, Dongho Wonc, Hyoungshick Kimc, Youngsook Lee “A three-factor anonymous user authentication scheme for Internet of Things environments” ELSEVIER 2020.
15. Anca Jurcut, Tiberiu Niculcea, Pasika Ranaweera, Nhien-An Le-Khac “Security Considerations for Internet of Things: A Survey” SN Computer Science 2020.
16. Chi-Tung Chen, Cheng-Chi LeeID, Iuon-Chang Li “Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments” PLOSE ONE 2020.
17. Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, and Peng Li “SKINNY-Based RFID Lightweight Authentication Protocol” MDPI 2020.
18. Evangelina Lara, Leocundo Aguilar, Mauricio A. Sanchez, and Jesús A. García “Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things” MDPI 2020.
19. Afrah Albalawi, Amal Almrshed, Arwa Badhib, Suhair Alshehri “A Survey on Authentication Techniques for the Internet of Things” IEEE 2019.
20. Seul-Ki Choi, Ju-Seong Ko, Jin Kwak “A Study on IoT Device Authentication Protocol for High Speed and Lightweight” IEEE 2019.