Maintain CIA of internal network in IoT

Ms. Shah Bhavisha[1] Mr. Aditya Kumar Sinha[2] Mrs. Vineeta Tiwari[3]
[1]Research Scholars
[1]GTU PG School, Gandhinagar, India [2,3]CDAC ACTS, Pune, India

Abstract— Now a day's very emerging paradigm, IoT is become an indispensable part of our life for comfort and automation in our day to day life. But, with the increasing use of internet, security issues related to that are also an essential part to maintain confidentiality and integrity of data in communication. In IoT, IP enabled wireless sensor node are directly connected with gateway and internet. So, securing data communication here, we proposed one protection preserving system and it is secure authentication system as well as encryption of outgoing sensed data. This system is working between gateway and sensor node for authorizing the sensor node by the gateway. This system is also beneficial for achieving integrity and confidentiality of data and also preventing from the different kind of security attacks likes compromised node attack, etc.

Key words: IoT, security challenges, IP enabled sensor node, Authentication, Encryption, and security attacks

I. INTRODUCTION

Recent advances in wireless technology for communication and computing leads to fully automated system in people's day-to-day life, and for this kind of automation system emerging technology is Internet of Things.

Through IoT we can extend Information Technology (IT) for our lives. IoT transforming current isolated network and infrastructure into a global network of interconnected objects. IoT means the interconnecting deice with their unique identity in the Internet. IoT working on different protocols, standards and mediums with layering approach. IoT includes devices with various sensing, measuring and data capture ability with that achieve identification, location, monitoring and management of interconnected devices.

This all features are done in various stages such that sensing, gathering of information and transform for further computation through any transmission network [1]. But, these all stages are vulnerable to different security attack especially due to direct connectivity with the internet. This vulnerabilities leads to different security attacks as well as also leads to authentication, access control, data privacy kind of issues [10]. So, if we combine and concerning all security issues to enhanced security of IoT, IoT devices is the best and very easy solution for our comfort in terms of controlling and managing things from one place towards the globe and its available with cheaper price[2].

So, for enhancement of security in IoT network here, we proposed on protection preserving system to maintain CIA characteristics of data security. For that this proposed system does authorization and encryption of data.

In this paper the further sections are arranged like section 2 is concerned with literature survey and finding the challenges, section 3 is concerned with proposed architecture and flow of system, section 4 is concerned with results and analysis and it shows how the proposed system should be work with and how much it should be beneficial for maintain security, last section 5 is presents the conclusion of this paper.

II. RELATED WORK

In this section, the related works from literature on maintain CIA with authentication with concern of security. As our work is specifically related to IoT, their security challenges and authentication of IP-enabled sensor node [3].

There are many security issues in concern of IoT in terms of authentication, access control, data privacy, securing a transmission network and various kinds of security issues [9]. Some of the major issues are as following:

1) IoT devices that provide user interfaces were vulnerable to a range of issues such as persistent XSS and weak credentials.
2) IoT devices along with their cloud and mobile applications components failed to require passwords of a sufficient complexity and lengths.
3) IoT devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.
4) IoT devices used unencrypted network service.
5) IoT device collected at least one piece of personal information via the device, the cloud or its mobile application.
6) Insufficient authentication and authorization.
7) Insecure web interface.
8) Lack of transport encryption.
9) Insecure software and firmware.
10) Information security and data privacy protection because of mobility, deployment and complexity.

Authentication is most important aspect of any IoT device [11]. If authentication is not proper then it leads the issues related to the privacy of sensitive and important data, it also harmful for the whole infrastructure of the IoT because any one can easily get authorized access through creating backdoor or with the breaking of authentication [4]. Some issues with authentication are as following [7]:

1) Node deployment There are two type of node deployment such that
– Static deployment,

– Dynamic deployment.

Static deployment is vulnerable for replay attack [4]. If deployed node should be traceable than we can find replay attack and take counter act against it but, if node can't be traceable for authentication following issues should be face [12]:

– Moving nodes re-authentication.
– Nodes movement that should be untraceable.
– Message integrity.
– Confidentiality.
– Node capture and compromise.

2) Complex management of public key infrastructure.
3) Computational bottleneck.
4) OAuth authentications have been bound with HTTP only.

In IoT, there is no standardized authentication mechanism at gateway for authenticating sensor nodes [5]. So, every IoT application vendors are used any of the authentication mechanism which are available in cryptographic information security world such as Kerberos, X.509, RFID based authentication, PAP, Host identification protocol, etc [6]. Those all authentication systems are patented and standard authentication as per the cryptographic view but, still they all having their own limitation in terms of security from the various kind of security attacks i.e. DoS attack, Impersonation attack, data theft attack, Flooding attack, etc [8].

So, for the preserving authentication system from these kind of issues implements some protection mechanisms which are either for identifying the attacks affected sensor node or protecting from the affection of the attacks from the sensor node side.

III. PRPOSED MODEL

IoT is working on different protocol and standards. So security features will also be fit with any of the protocol and standard. Existing solutions are not feasible with all of the protocols, and if feasible then it is very complex and energy consuming or there may have leaking part of security. Here, I proposing protection preserving system for secure authentication and it will feasible with all protocols and standards and also not too much complex and energy consuming. This proposed system first checks the outgoing packets from the sensor node at gateway and only valid packets have been gone for further process.

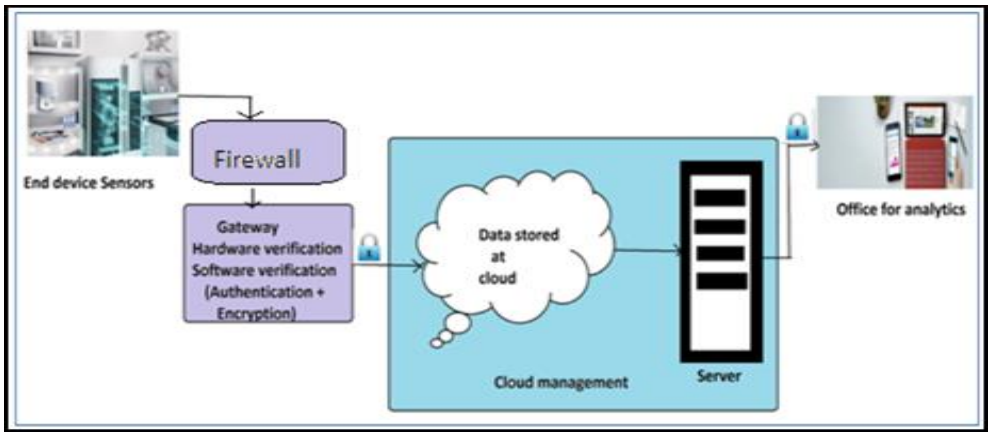

Fig. 1: Proposed model architecture

As shown in Fig.1 the proposed system is implemented before the gateway. After verifying the packets whether it is valid or invalid the packets forward towards the gateway and the actual authentication are done. Working of proposed system is as shown in Fig. 2.

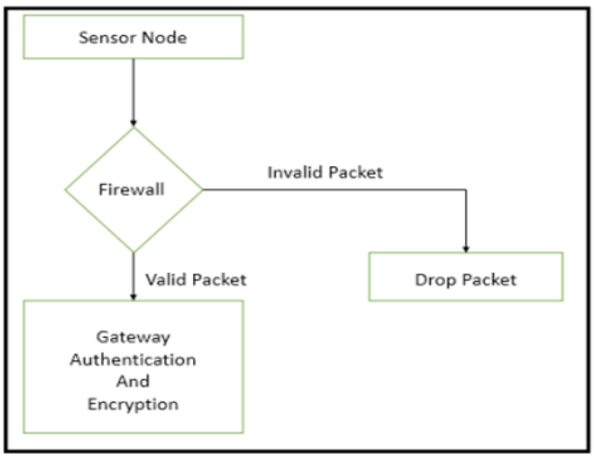

Fig. 2: Flow of Firewall

After verifying the packets at firewall the packets should be allowed towards the gateway and at gateway the actual device authentication process is done which we have been proposing for gateway authentication. For gateway authentication we propose the modified Kerberos network authentication protocol and try to removing the limitation of that protocol. The major changes are initiation of request, No. of servers required, encryption technique and key establishment in main Kerberos network authentication protocol. Working of proposing authentication mechanism is as shown in Fig. 3.

So In our proposed system, with the help of firewall we analyze the packet should be malicious or real and with the help of gateway authentication verifies the device is compromised (malicious) or not.

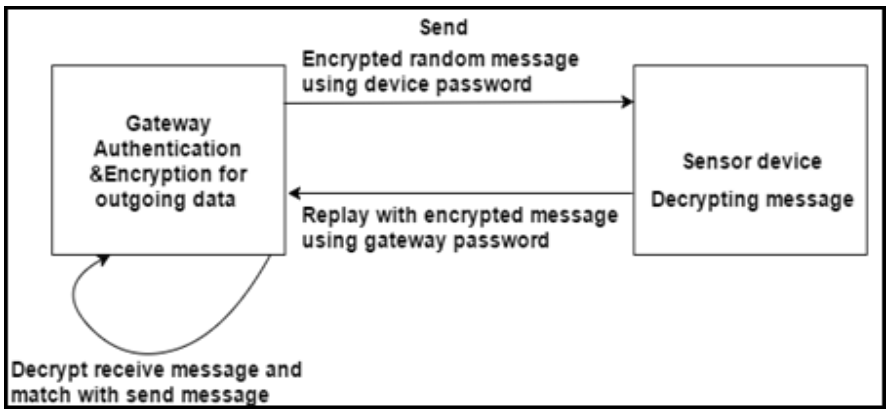

Fig. 3: Block diagram

Working of proposed device authentication system:

Step: 1 Gateway sends a random message in encrypted form and message is encrypted with store device password to the sensor device. For encryption process is done using symmetric lightweight AES encryption algorithm.

Step: 2 Device receives the message and decrypt it using their own password. This password is shared with gateway at the time of registered themselves with their IP address. And again encrypted with gateway password as a key using lightweight AES algorithm and send back to the gateway.

Step: 3 Gateway waits for the reply from device.

Step: 4 after getting reply from the device decrypt whole message and verifies decrypted random message is same as send random message and key.

Step: 5 If both matches device node will authenticate otherwise it should be compromised. Compromised node should blocked by their IP address and deny the data flow from that device.

Step: 6 with authentication process are completing the device should start transmission of data in encrypted form towards the gateway. For encryption of data the random message is key and used lightweight encryption method.

Step: 7 Gateway checks the device authentication; if device is within time-stamp then it should be authenticated if not then starts with Step: 1.

In this proposed mechanism at the time of installing device into network one key is pre stored for encryption purpose and after authentication process every time new key is established for encryption. Data transmission is also in encrypted with that stored or newly established key. This encryption is done with lightweight AES encryption algorithm.

IV. RESULT & ANALYSIS

For implementing the proposed scenario in IoT environment we used Raspberry Pi board with temperature sensor as a sensor device and used a gateway as a PC.

For the analysis of checking the efficiency of proposed system we consider time, security, number of nodes as a parameter.

Following image are shown the process of proposed system.

Fig. 4: Client Process

Above Fig. 4 shows the sensor device process for authorizing at gateway.

Fig. 5: Gateway Process

Fig. 5 shows the server process for authenticating the sensor device.

Fig. 6: Sensed Data at gateway

Fig. 6 shows the after authentication process sensed data received at gateway.

Here, we also checks the time for authentication with lightweight AES with increasing number of nodes.

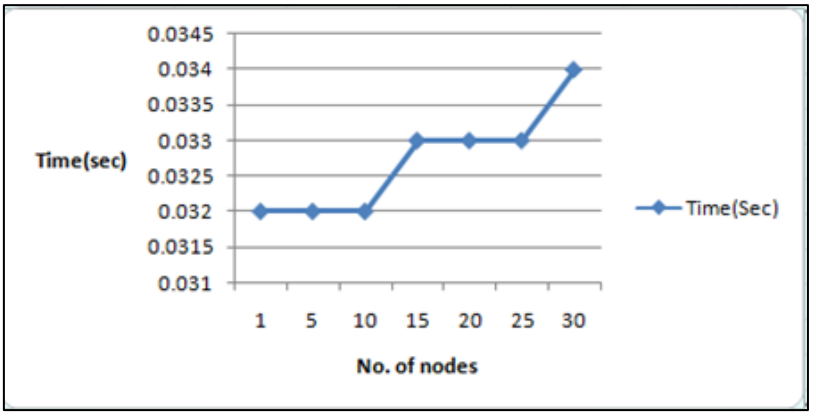

Fig. 7: No. of nodes v/s Time (Sec)

According to graph we can show that time is almost same for authorizing process.

V. CONCLUSION

IoT is good paradigm for our day-to-day life comfort. But, Security issues are also matter with IoT. Proposed solution is feasible with all types of IoT protocols and standards. Using this proposed solution we can monitor the packets and their containing data and also verifies whether it is coming from the authorized node or from the affected node. So, proposed solution is also helpful for the identifying affected node through any kind of security attacks. This proposed system is very light weighted and also reduces the consumption of power, and increases the battery life time.

REFERENCES

[1] Mian Ahmad Jan, Priyadarsi Nanda, Xiaangjian He, Ren Ping Liu "A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment," pages 205 – 211. IEEE, 2014.
[2] Christial Gehrmann, Marco Tiloca, Rikard Hoglund " SMACK: Short Message Authentication ChecK against Battery Exhaustion in the Internet of Things," pages 274 – 282. IEEE, 2015.
[3] Ola Salman, Sarah Abdallah, Imad H Elhajj, Ali Chehab, Aymann Kayssi "Identity-Based Authentication Scheme for the Internet of Things," IEEE, 2016
[4] Sudha Patel, Dhiren R. Patel, Ankit P. Navik "Energy Efficient Integrated Authentication and Access Control Mechanisms for Internet of Things," pages 304 – 309. IEEE, 2016.
[5] Fan Wu, Lili Xu, Saru Kumari, Xiong Li" A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," Springer, 2016.
[6] Hong Yu, Jingsha He " Authentication and En-route Data Filtering for Wireless Sensor Networks in the Internet of Things Scenario," Vol. 6, No. 1, pages 1 – 12 International Journal of Grid and Distributed Computing, 2013.
[7] Yaman Sharaf- Dabbagh, Walid Saad " On the Authentication of Devices in the Internet of Things," IEEE,2016
[8] Aimaschana Niruntasukrat, Chavee Issariyapat, Panita Pongpaipool, Koonlachat Meesublak, Pramrudee Aiumsupucgul, Anun Panya" Authorization Mechanism for MQTT-based Internet of Things," IEEE, 2016.
[9] S. Raja Rajeswari, V. Seenivasagam "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," Volume pages 16. Scientific World Journal, 2016.
[10] Keyur K. Patel, Sunil M. Patel " Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges," Volume 6 Issue No. 5 pages 6121 – 6133. IJESC, 2016.
[11] DocPlayer Protocol-stack URL http://docplayer.net/docs-images/30/14676721/images/12-0.png
[12] Hewlett Packard "Internet of Things Report" 2015.