Secure Authentication, Contract and Communication for IoT Environment using MQTT Protocol

Hariprasanna M.A.
PG Student
Dept. of CS&E, S. J. College of Engineering
JSS Science and Technology University
Mysore, Karnataka, India

P. Mahesha
Asst. Professor
Dept. of CS&E, S. J. College of Engineering,
JSS Science and Technology University
Mysore, Karnataka, India

ABSTRACT

Internet of Things (IoT) is a subject of ample interest and it is a current technology. In last few years, security of the IoT systems is a field of wonderful research activities. Mutual authentication between the IoT devices and Users of IoT Environment is a significant part of secure IoT systems. Widely used authentication mechanisms, which are Single password based, are vulnerable to the side-channel and dictionary attacks. In this paper, multi-key based mutual authentication mechanism to provide a secure authentication, contract and communication between the IoT devices and Users of IoT Environment is introduced. In this approach, the publish-subscribe based Message Queuing Telemetry Transport (MQTT) protocol is used for secure communication, which is bandwidth-efficient and uses small amount of battery power. Using the Blockchain technology to store data helps to bring trust and transparency in the developed model. In order to demonstrate this entire methodology, authors have created a prototype using NodeMCU IoT platform for IoT Environment. The NodeMCU IoT platform is used for making effectual and fast IoT applications. The goal is to provide a secure authentication, contract and communication for IoT Environment. It is satisfactorily achieved with good response time as authenticated user can only be able to access control the IoT device.

General Terms

IoT, Security, Blockchain

Keywords

IoT Device, Users of IoT Environment, Message Queuing Telemetry Transport (MQTT) protocol, Adler-32

1. INTRODUCTION

In the globe of the IoT, billions of devices are linked to the Internet and that gives an attacker a chance to control the IoT system on a huge scale. The IoT has become a rising subject recently. It can be defined as the connection of devices or things over the internet to convey upon a given function. This primarily comes as devices sending or collecting information. Because of the entry of super-cheap computer chips and the universality of wireless systems, nowadays it is possible to turn anything, from something as little as a pill to something as large as an airplane, into a part of the IoT. The IoT is making the fabric of the globe around us more brilliant and more reactive, blending the digital and physical universes. Essentially, it is possible to transform any physical object into an IoT device if it can be connected to the internet, to be controlled or want to communicate the data. Authentication, authorization, data confidentiality and privacy are some of the significant security problems of IoT.

2. LITERATURE REVIEW

One of the approach [1, 5, 6] proposed by the researchers is the use of a secure authentication protocol to authenticate the IoT device and the server. The existing authentication mechanisms, which are primarily based on single password, are exposed to dictionary and side channel attacks. A multi key authentication mechanism is designed and token values will be changing over the time, which avoids dictionary attacks [1, 5, 6].

Kalra S and Sood S. K [2] introduced the IoT authentication and key agreement scheme. Even though the authors' method uses the elliptic curve cryptography to improve the security, it has two security issues; they are the mistiness of the session key and the failure of mutual authentication [2, 7].

Hao Zhang and Tingting Zhang [3] present the framework to design a security protocol for the IoT. In this approach, authors' framework gives the information about the structure, philosophy and communication of the security protocol. This mechanism is implemented on the SensibleThings platform and provides communication for the devices connected to the IoT [3, 8, 11].

Randa Almadhoun et al. [4] present a user authentication scheme using blockchain enabled fog nodes. In this technique, users are authenticated to access IoT devices by fog nodes interface to Ethereum contracts. The fog nodes are used to deliver scalability to the system by relieving the IoT devices from carrying out heavy computation involving tasks related to authentication and communicating with the blockchain. Additionally, blockchain has developed as technology with capacities to give secure authentication, management and admittance to IoT devices and their information [4, 9, 10, 12].

As per the observation there is very limited work proposed using Blockchain for IoT devices. Also, the limited work on the Contract based communication with hashing technique between the users and IoT devices is proposed in the previous works.

3. PROPOSED SYSTEM

The implementation involves the following methodology to develop a secure platform for IoT Environment

- Authentication
- Contract
- Communication

Following subsections show steps followed in each one of these phases and these phases are pictorially represented in Figure 1.

3.1 Authentication Phase

i. User device and user profile management
ii. Data security key generation
iii. Distribution and mapping user profile with keys
iv. Accept user request
v. Get secret key (Sk) from Secure Vault for the user (U), represent as U_{Sk}
vi. Encrypt using key to generate Secure key E_{Usk}
vii. Share Secure key to user E_{Usk}
viii. User should Decrypt E_{Usk} to identify key and return back D_{Usk}
ix. Validate E_{Usk}==D_{Usk}, identify user as valid user to create contract

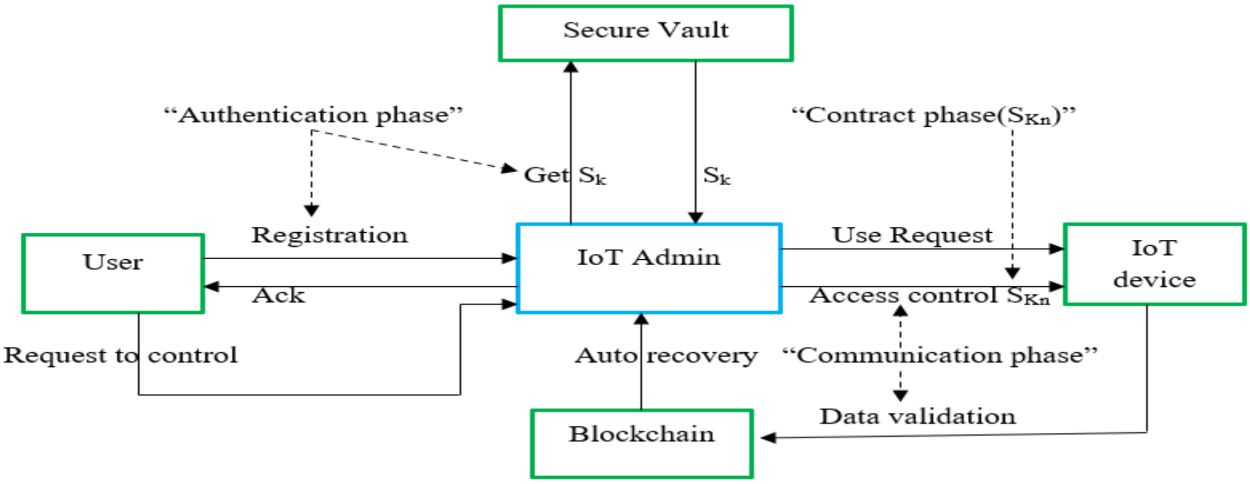


Figure 1: Architecture Diagram of the Proposed System

3.2 Contract Phase

i. Contract is a session key S_{Kn} for valid user post authentication phase.
ii. Server should distribute S_{Kn} for user and IoT environment for any further transaction.
iii. S_{Kn} assigned with timeout for the contract and expired automatically based on timeout.

3.3 Communication Phase

i. User request is always attached with S_{kn} for any transaction.
ii. Secure communication via cloud created for the client to control IoT devices and same will be stored using blockchain technology for future data validation.
iii. The MQTT protocol is used for communication between the IoT device and Users of IoT Environment.
iv. Communication phase should be active until Session Key gets expires.

3.4 Message Queuing Telemetry Transport protocol

The MQTT is a messaging protocol based on the publish-subscribe technique. Publishing of messages and subscribing to topics or "pub/sub" is the principle on which the MQTT protocol is built. Many clients link to a broker and subscribe to the topics that they are concerned in. Same topics can be used to subscribe for many clients and clients can access the data as they please.The MQTT protocol and a broker acts as a simple and common interface for everything to link to.The default port for MQTT is 1883 and it is registered for secure MQTT. In the proposed work, authors have implemented the MQTT protocol between the user and IoT device for message exchange.

HiveMQ is one of the MQTT brokers. It is a service provider, which uses the MQTT protocol for efficient data exchange between the user and IoT Environment. Authors have integrated the HiveMQ and MQTT broker in the proposed system.

3.5 Adler-32 Algorithm

Hash is created for each entry in the Blockchain ledger. In order to create hash, authors use Adler-32 algorithm. It is a popular checksum algorithm designed to detect corruption in the data. Since it is faster than the other checksum algorithms, Adler-32 is chosen for the current work. If the uncompressed information does not match with the Adler-32 checksum, the application can notify its protocol or the handler that the information is corrupted.

In order to get an Adler-32 checksum, we have to calculate the two 16-bit checksums P and Q and adding their bits into a 32-bit integer. P is the aggregate of all bytes in the stream in addition to one and Q is the aggregate of the individual values of P from each phase.

At the start of an Adler-32 run, P is set to 1, Q to 0. The sums are done modulo P_n(the highest prime number). The bytes are stored in network order, Q occupying the two most significant bytes.

An Adler-32 function can be explained as

$$P= 1 + Z_1 + Z_2 + \ldots + Z_n \ (\text{ mod } P_n)$$

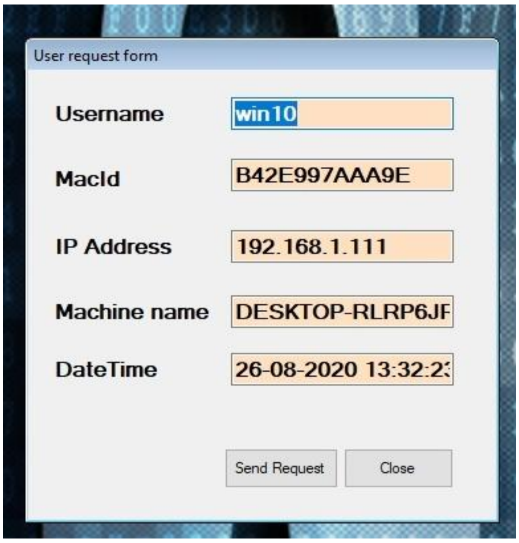
$$Q= (1 + Z_1) + (1 + Z_1 + Z_2) + \ldots + (1 + Z_1 + Z_2 + \ldots + Z_n) \ (\text{ mod } P_n)$$

$$Q= n*Z_1 + (n-1)*Z_2 + (n-2)*Z_3 + \ldots + Z_n + n \ (\text{ mod } P_n)$$

$$\text{Adler-32}(Z) = Q*(P_n + \text{Checksum}) + P$$

where Z is the string of bytes for which the checksum is to be calculated, P_n is the highest prime number and n is the length of Z.

4. EXPERIMENTAL RESULTS



User request form

Username: win10

MacId: B42E997AAA9E

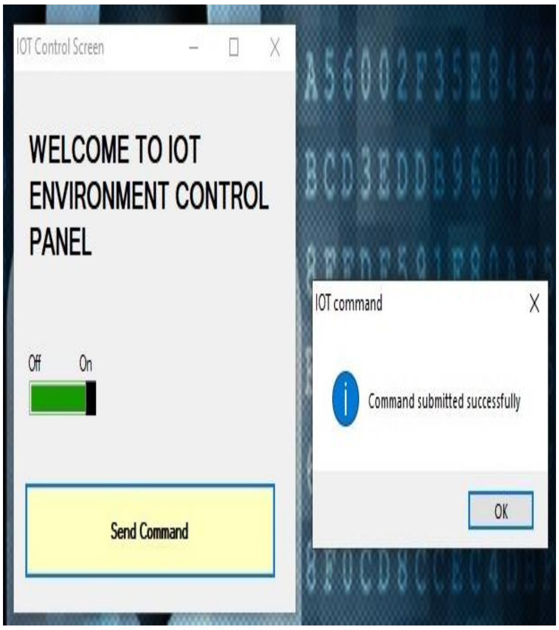
IP Address: 192.168.1.111

Machine name: DESKTOP-RLRP6JF

DateTime: 26-08-2020 13:32:2:

Figure 2: User Request

The Figure 2 describes the User Registration Request form containing attributes such as Username, IP address, Mac ID, Machine name, Date and time. The user information is auto fetched from the system and request is sent to the administrator.



IOT Control Screen

WELCOME TO IOT ENVIRONMENT CONTROL PANEL

IOT command

Command submitted successfully

Figure 3: IoT Control Screen

The IoT Environment Control Panel is pictorially shown in Figure 3.When the admin grants the permission to access the IoT device, the control screen will be displayed. Turn On the button and send command to the IoT Environment then the message is displayed as “Command Submitted Successfully” and the LED light will be On in the model.

Table 1. Comparison of MQTT Protocol with HTTP Protocol

1000 Messages	**Average Time in Seconds**
MQTT (1publish-subscribe per message)	5.9
HTTP (1 POST-GET per message)	115.6

The Table 1 shows the tabulation of values obtained after comparing the performance parameters of MQTT protocol with HTTP protocol in terms of average time taken in seconds. Experiment is repeated for 1000 messages and average time is tabulated.

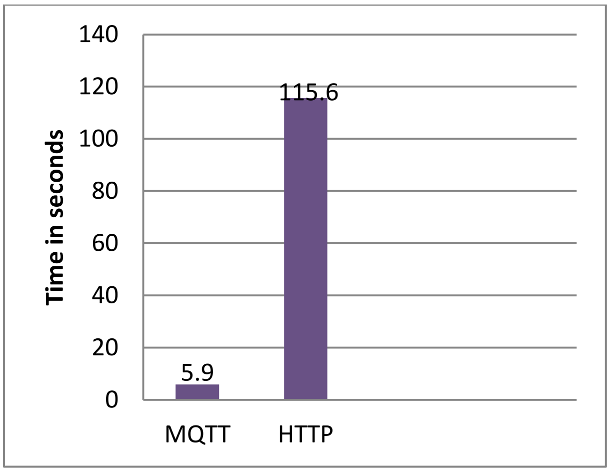


Figure 4: Comparison of MQTT Protocol with HTTP Protocol

The Figure 4 shows the pictorial representation of values tabulated in Table 1. The MQTT and HTTP protocols have taken 5.9 and 115.6 seconds respectively. It is found that the MQTT protocol is faster than HTTP because of short message header and 2 bytes of packet message size.

Table 2. Proposed System’s Average Response Time vs. No. of Users

No. of Users	**Average Response Time in Seconds**
1	1.35
2	1.59
3	1.74
4	1.78
5	1.80

The Table 2 shows the tabulation of average response time in seconds when no of users are different.

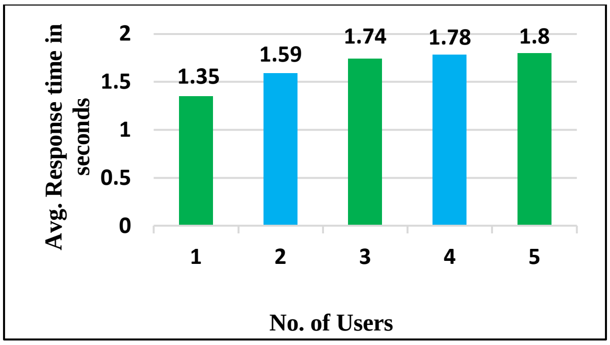


Figure 5: Proposed System Average Response Time vs. No. of Users

The average response time with respect to number of users is pictorially shown in Figure 5. The average response time is satisfactory, even when the number of users is more.

5. CONCLUSION

In this paper, authors have introduced a mechanism to provide a secure authentication, contract and communication between the IoT device and Users of IoT Environment. The set of Secret keys in Secure Vault are keep changing after each successful communication session between the user and IoT device. The model uses MQTT protocol for communication between the IoT device and Users of IoT Environment. The information is stored using Blockchain technology for future data validation.

Proposed system is implemented and tested to ensure Secure IoT communication between user and IoT device using authentication, contract, communication and data validation.

Developed application is tested to check for side-channel and dictionary attack by verifying user certificate on unauthorized machine to show unsuccessful communication between user and IoT Environment.

In future the model can be further improved by storing the data at servers that are at different geographical location.

6. ACKNOWLEDGMENTS

Authors are thankful to the management of the university.

7. REFERENCES

[1] Trusit Shah and S. Venkatesan, “Authentication of IoT Device and IoT Server Using Secure Vaults”, In Proceedings of 17th IEEE International Conference, New York, USA, pp. 819-824, 2018.

[2] Kalra S and Sood S. K, “Secure Authentication Scheme for IoT and Cloud Servers”, Journal of Pervasive and Mobile Computing, Elsevier Publications, Vol. 24, pp. 210-233, 2015.

[3] Hao Zhang and Tingting Zhang, “A Peer to Peer Security Protocol for the Internet of Things”, In Proceedings of 18thIEEE International Conference, Paris, France, 2015.

[4] Randa Almadhoun, Maha Kadadha and Maya Alhemeiri, “A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes”, In Proceedings of 15th IEEE International Conference, Aqaba, Jordan, pp.1-8,2018.

[5] Hittu Garg and Mayank Dave, “Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware”, In Proceedings of 4th IEEE International Conference, Ghaziabad, India, pp. 1-6, 2019.

[6] Alok Kumar Gupta and Rahul Johari, “IOT based Electrical Device Surveillance and Control System”, In Proceedings of 4th IEEE International Conference, Ghaziabad, India, pp. 1-5, 2019.

[7] Jun Suzuki, Akira Tsuji, Yuki Hayashi, Masaki Kan and Shinya Miyakawa,“Device-Level IoT with Virtual I/O Device Interconnection”, In Proceedings of IEEE International Conference, Luxembourg City, Luxembourg, pp. 67-74, 2016.

[8] Shapna Muralidharan and Heedong Ko, “An Inter Planetary File System (IPFS) based IoT framework”, In Proceedings of IEEE International Conference, Las Vegas, NV, USA, USA, pp. 1-2, 2018.

[9] Madhusudhan Singh, Abhiraj Singh and Shiho Kim, “Blockchain: A Game Changer for Securing IoT Data”, In Proceedings of 4th IEEE International Conference, Singapore, pp. 51-55, 2018.

[10] Hien Thi Thu Truong, Miguel Almeida, Ghassan Karame and Claudio Soriente, “Towards Secure and Decentralized Sharing of IoT Data”, In Proceedings of IEEE International Conference, Atlanta, GA, USA, pp. 176-183, 2019.

[11] Seul-Ki Choi, Ju-Seong Ko and Jin Kwak, “A Study on IoT Device Authentication Protocol for High Speed and Lightweight”, In Proceedings of IEEE International Conference, Jeju, Korea(South), pp. 1-5, 2019.

[12] Sarada Prasad Gochhayat, Eranga Bandara, Sachin Shetty and Peter Foytik, “Blockchain based Encrypted Cloud Storage for IoT Data”, In Proceedings of IEEE International Conference, Atlanta, GA, USA, pp. 483-489, 2019.