Secured Certificate Based Authentication

Madhura S Patil, Priyanka R Megharaj, Sindhu V, Sushma H S, Sowmya M*

Department of CSE, GSSSIETW, Mysuru, Karnataka, India

DOI: https://doi.org/10.21467/proceedings.1.25

* Corresponding author email: sowmyam@gsss.edu.in

Abstract

A Secured Certificate based authentication does not require passwords or tokens, instead digital certificates are used to solve authentication challenge. In this paper we are discussing design and implementation of security protocol for the IOT. Admin will generate a digital certificate and multiple keys for a valid user using SHA. The certificate and keys are downloaded by user. The user will communicate with admin through digital certificate for the secured authentication of IOT.

Index Terms- Registration, Approval, Certificate Generation and Sharing, Request to access, Certificate and Secure Key, Authentication, Control to Access.

1 INTRODUCTION

The Internet of Things is the network of physical objects embedded with electronics software, sensors and network connectivity, which enables these objects to collect and exchange data. The IOT can find applications in many fields such as smart health care, smart agriculture, smart grid, building management, etc. The powerful embedded devices such as smart phones and tablets will occupy the great part of the IOT. The different devices not only bring various applications but also limitations in terms of reliability, information leakage, privacy and security issues. It makes difficult to implement complex security protocols in order to protect the system and the information. The project focuses on the development of a security protocol which provides an efficient authentication mechanism. The security protocol is implemented by using Secure Hash Algorithm (SHA). A private cloud server can be set up in a Raspberry Pi which could be used as a storage device for the applications.

Cloud storage is a backend server which provides seamless scalability and it removes the necessity of operating data bases which are distributed in nature. Cloud stores large amount of data centrally and also it is able to provide access to restricted users via the internet across different geographical regions just by connecting into the same network. The Raspberry Pi is a series of credit card sized single-board computers developed by the Raspberry Pi Foundation. Raspberry Pi is a cheaper microprocessor in which cloud computing infrastructure can be obtained using cloud platforms.

2 LITERATURE SURVEY

This [3] paper resolves authorization requests for constraint devices when user wants to access any of devices data or services. The authorization engine is exposed through API and therefore most of the IOT devices can access it. The proposed method is very complex frame work built on top of the existing technologies. However, they deal with user device security this work does not address machine to machine trust. [4] This paper describes framework for data authenticaton in IOT. Data are treated as streams with security puncactutations, which get analyzed before the data are provided to its consumers. The work does not describe how to apply security rules therefore MAC, DAC and RBAC can apply for such solution. Nevertheless, the work expects the data creator to set restrictions on them, which is unsuitable in many applications when the sensor is just a slave of another hierarchically, a higher entity. It does not address problem of security rules duplication and consistency across different devices. [2] This paper uses capability of tokens for granting access to services. The token is issued by provider for a client during the initial provision of a service. It consists of URL, user/object ID, time stamp of creation, subscription period, service ID and list of access permissions.

3 PROPOSED METHOD

The paper proposes the method of implementing the security protocol for sensible things platform. The protocol will not only cover the integrity of messages, but also the authentication of each user by providing an efficient authentication mechanism. The secured authentication is implemented by the following steps.

2.1 Registration Request

2.2 Approval Process

2.3 Certificate Generation and Sharing

2.4 Request to Control

2.5 Control to Access

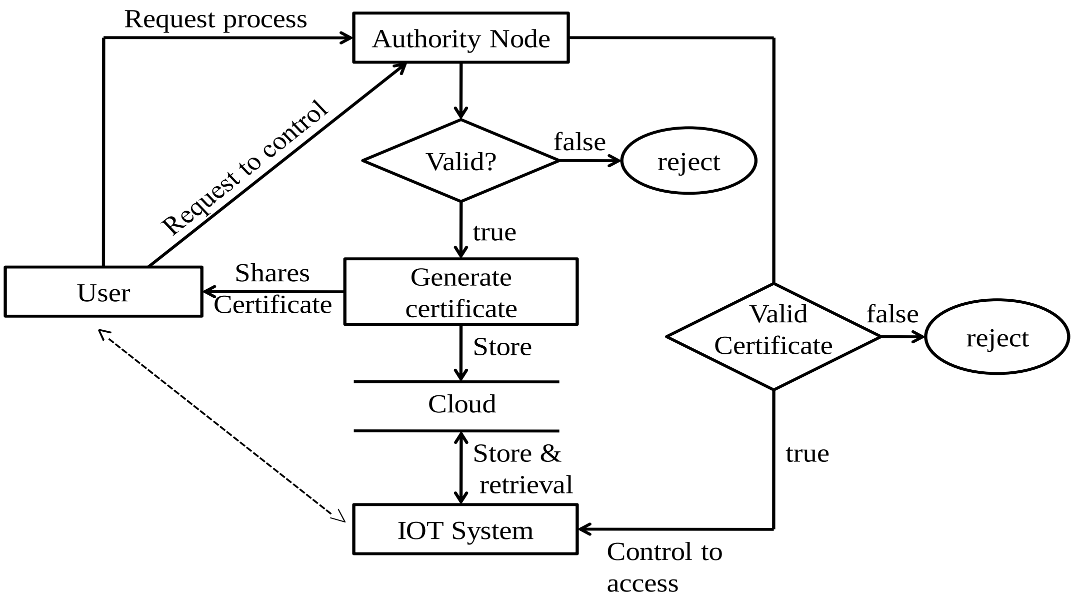


Figure: Secured Authentication

3.1 Registration Request

The Registration Process is carried out between User and Admin. The user will send a request to admin, in which all user information such as, Username, Mac ID, IP address, Machine name, Date and Time will be auto fetched and filled into registration form and the request is sent to admin. The registration form is in read-only method, no intruder can edit the user information.

3.2 Approval Process

During approval process, the registration request details are stored in cloud database and this request will be waiting for Admin approval. The admin will take-up the request from the cloud database, if it is valid request the admin will approve the request otherwise the request is deleted.

3.3 Certificate Generation and Sharing

The admin will take up the combination of user information that is username, Mac ID, IP address, machine name and is given to SHA. This algorithm generates a cipher text and is used to generate a digital certificate. The private and public keys are generated by RSA.

The user will have an option of checking his approval status. If the request is approved by admin, he can download a certificate and a private key from cloud data base.

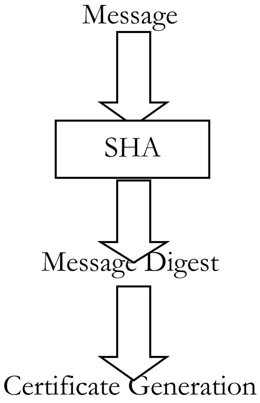


Figure: Generation of Certificate using SHA

3.4 Request to Control

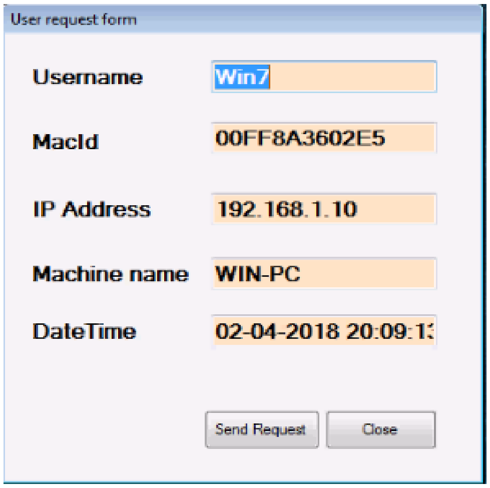
The user will send a request to admin along with certificate. The cloud server will compare the send certificate with stored certificate to verify whether the request is from the same user or not. If both certificate matches it will generate OTP, encrypted by public key and is send to user. User will decrypt this token by private key and he will send the OTP. If both OTP are same, admin will generate a session key and is given to user.

3.5 Control to Access

The user will send a request and session key to IOT system. As long as the session key exists, the user can control the IOT. Once the session key expires he has to send a request again.

4 RESULT

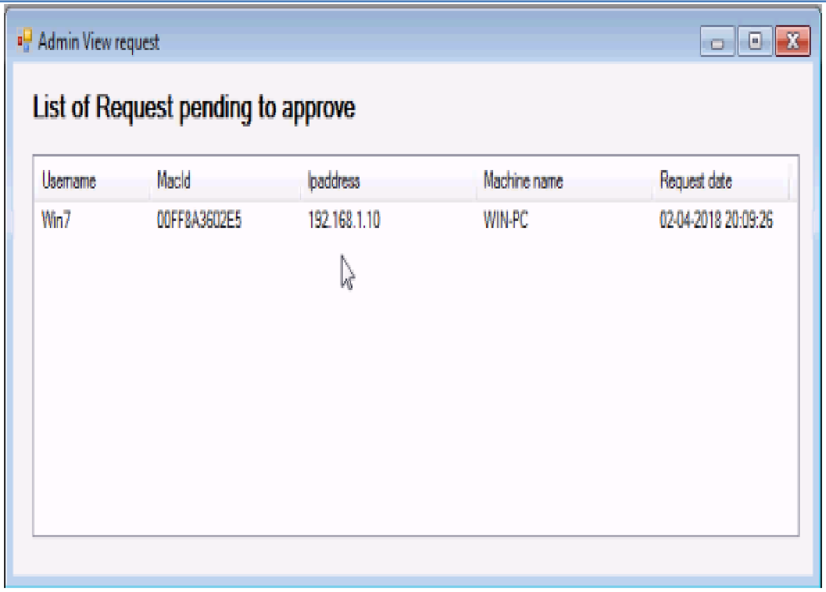
The results of secured certificate-based authentication are shown below



User request form

Username	Win7
MacId	00FF8A3602E5
IP Address	192.168.1.10
Machine name	WIN-PC
DateTime	02-04-2018 20:09:1

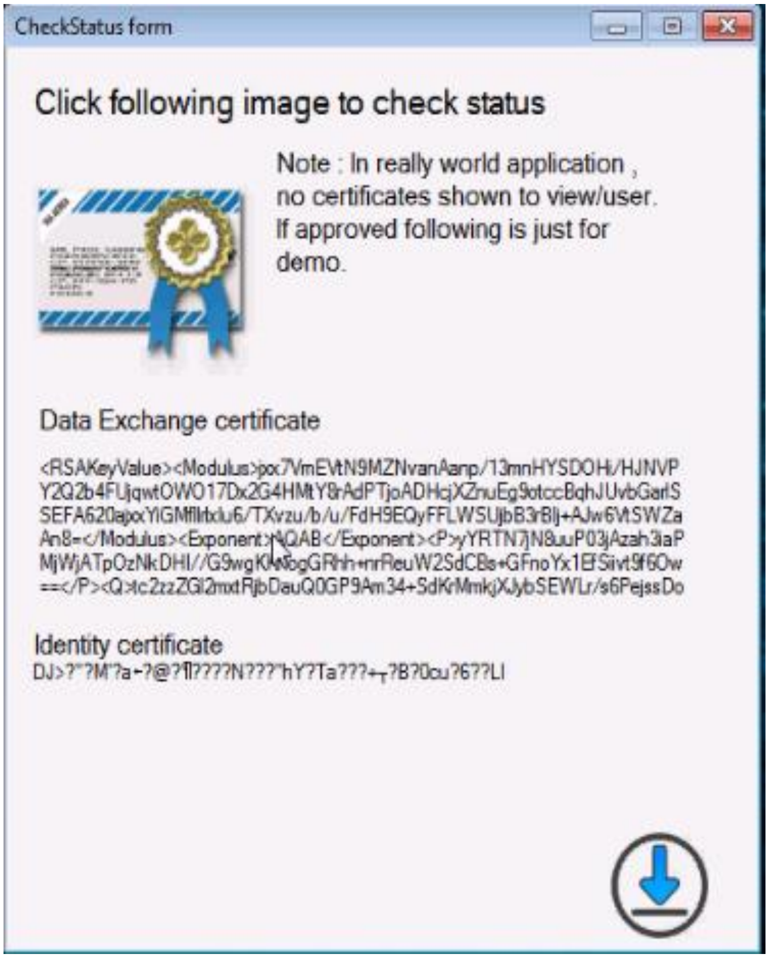
Figure 1. Registration Request



List of Request pending to approve

Username	MacId	Ipaddress	Machine name	Request date
Win7	00FF8A3602E5	192.168.1.10	WIN-PC	02-04-2018 20:09:26

Figure 2. Approval Process



Click following image to check status

Note : In really world application , no certificates shown to view/user. If approved following is just for demo.

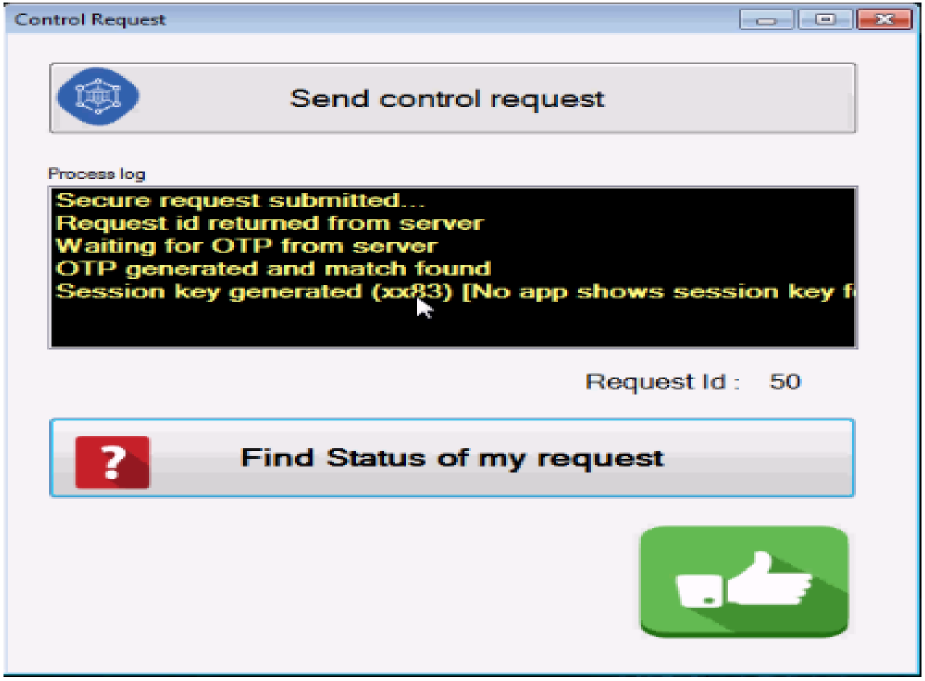
Data Exchange certificate

```
<RSAKeyValue><Modulus>pxx7VmEVtN9MZNvanAanp/13mnHYSDOHi/HJNVP
Y2Q2b4FUjqwtOWO17Dx2G4HMtY8rAdPTjoADHcjXZnuEg9otccBqhJUvbGarlS
SEFA620ajxxYiGMfllrbxlu6/TXvzu/b/u/FdH9EQyFFLWSUjbB3rBlj+AJw6VtSWZa
An8=</Modulus><Exponent>AQAB</Exponent><P>yYRTN7jN8uuP03jAzah3iaP
MjWjATpOzNkDHI//G9wgKNogGRhh+nrReuW2SdCBs+GFnoYx1EfSiivt9f6Ow
==</P><Q>tc2zzZGl2mxtRjbDauQ0GP9Am34+SdKrMmkjXJybSEWLr/s6PejssDo
```

Identity certificate

```
DJ>?"?M"?a-?@?¶????N???"hY?Ta???+┬?B?0cu?6??LI
```

Figure 3. Certificate Download



```
Secure request submitted...
Request id returned from server
Waiting for OTP from server
OTP generated and match found
Session key generated (xx83) [No app shows session key f
```

Figure 4. Request to Control Process

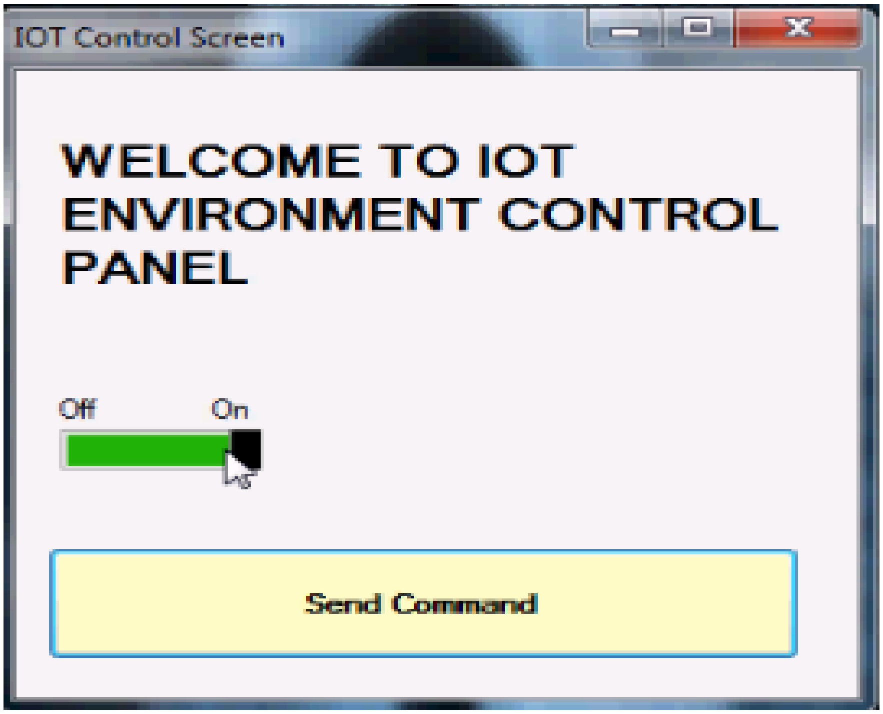


Figure 5. Control to Access

5 CONCLUSIONS

The IOT system have suffered from lack of reliability, security and privacy. In this project we have implemented the security protocol using SHA . The protocol not only covers the integrity of messages but also the authentication of each user by providing efficient authentication mechanism for IOT environment.

References

[1]. Sencun Zhu and Sammy Chan,"Distributed Access Control with Privacy support in Wireless Sensor networks", in 10 Oct 2011 Vol.10,No.10, in IEEE Transactions on Wireless Communication.

[2]. Pranatha ," A Distributed Secure Mechanism for Resource Protection in a Digital Echo System Environment" ,in 2012 Vol.3,No.1,Journal of Information Security.

[3]. Seitz, "Authorization Engine as Trusted Third Party", in 29 Dec 2015 IEEE International Conference on Internet Of Things.

[4]. Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet Of Things Technology for Comfortable Lifestyle", in 25 Dec 2015.

[5]. J.C Talwana and H.J. Hua," Smart World of Internet Of Things and its Security Concerns", in 2016, IEEE International Conference on IOT.

[7]. Trio Adiono, "Intelligent and Secured Software Application for IOT Based Smart Home", in 2017, IEEE 6th Global Conference.