SECURITY FOR IoT SYSTEMS USING MACHINE LEARNING

B N Kiran,Radheshyam S G, Sagar N,Sanath A Balthar,Shrinath

Assistant Professor, Department of Information Science and Engineering,The National Institute Of Engineering, Karnataka, INDIA

Student,Department of InformationScience andEngineering,The National Institute Of Engineering, Karnataka,INDIA

Student,Department of Information Science and Engineering,The National Institute Of Engineering,Karnataka, INDIA

Student,Department of Information Science and Engineering,The National Institute Of Engineering,Karnataka, INDIA

Student,Department of Information Science and Engineering,The National Institute Of Engineering,Karnataka, INDIA

Abstract

IoT(Internet of things) represents the systems which are connected by number of devices, having sensors and actuators by wired or wireless network. More than 30 million of devices will be connected together by 2025, IoT is one of the technology, which is rapidly growing in the last decade. One of the weakest part in IoT is the "security". IoT systems lacks the security for the data they collect, store & share over the network. Providing the security has become a major challenge. Securities such as preventing the unauthorized access of data, handling overloading of requests for access by authorized user. To approach these challenges for implementing secured IoT environment, we propose a centralized system for allowing only authorized user to access the IoT systems, using cryptography and analyse and maintain logs of the user activity with centralized system and IoT system environment using machine learning.

Keywords:- *Cloud server, IoT security, Authentication of client, Machine learning algorithm*

1 INTRODUCTION

The term Internet Of Things" for the first time was mentioned by Kevin Ashton in 1999 representing supply chain management aspects to the public[1]. The idea was so fascinating that it grew rapidly over past few years. IoT basic utilities are sensors and actuators, these kind of devices are low-resource devices. One more type of Iot device is gateway devices which uses less resources compared to edge devices. With more development of IoT devices data transfer between the devices increase then security of the data becomes an issue.There are several challenges with implementing security within an IoT network [3]. Security protocol isthe base of all system's communication and authentication. The Security protocol involves: Registration, Approval, Certificate generation, Certificate Sharing, Authentication and Control to access. To address this challenge in securing IoT devices, wepropose using machine learning within an IoT gateway to helpsecure the system. In this paper we are presenting an idea were the client which wants access permission of IoT device must register to the cloud using cryptography the client is authorized by the IoT system, machine learning algorithm is used to maintain logs of the client authorization failure. The idea of this concept is to provide security IoT system.

2 EXISTING SYSTEM

There are many IoT systems which provide access to the client without checking authorization here comes the security issue, the sensitive data can be lost in the network or data corruption occurs. Powerful embedded devices such as smart phones and tablets will occupy the great part of the IOT even these devices face privacy and security issues. It is easy to attack these embedded devices physically.The problem is that many devices use

wireless communication, which makes it easier to drop the messages.The aim here is to provide security to the data during the data transfer and prevent unauthorized client access using machine learning algorithm.

3 PROPOSED SYSTEM

This project concentrates on the design of a security protocol for the IOT.The core of the P2P security system for the Internet of Things is the security protocol. This protocol is the base of all system's communication and authentication. There are two mainparts in this security protocol: Registration, Communication.

4 ARCHITECTURE

We are developing a system security protocol for IoT. The clients which needs to access the IoT device must register in the first step, it communicates with authority node which in turn connected to cloud platform, cloud platform is used to store the clients information such as mac id, IP address and user name. The SHA algorithm is used to authorize the client by generating private and public key along with certificate for the client. The cloud system sends the private key back to the client this confirms the client registration, when client wants to access the IoT system it generates the request and send it to cloud if certificate of the client and generated certificate stored in cloud for that client matches OTP is generated and encrypts it with public key of that particular client and sends it to the client machine where decryption takes place with private key of it. The decrypted OTP is sent back to server it is matched again with the original OTP if no change is found session key is generated, which expires within certain period of time. Now the client machine has gained access to the IoT system, client sends SSH key along with the command that needs to be executed. Machine learning supervised algorithm used to ensure security, four type of failure logs are maintained.

1. Session key not yet generated
2. Session key mismatch
3. Network error
4. Certificate mismatch

If these type of failures has occurred during client system authentication those system access wiil be denied.

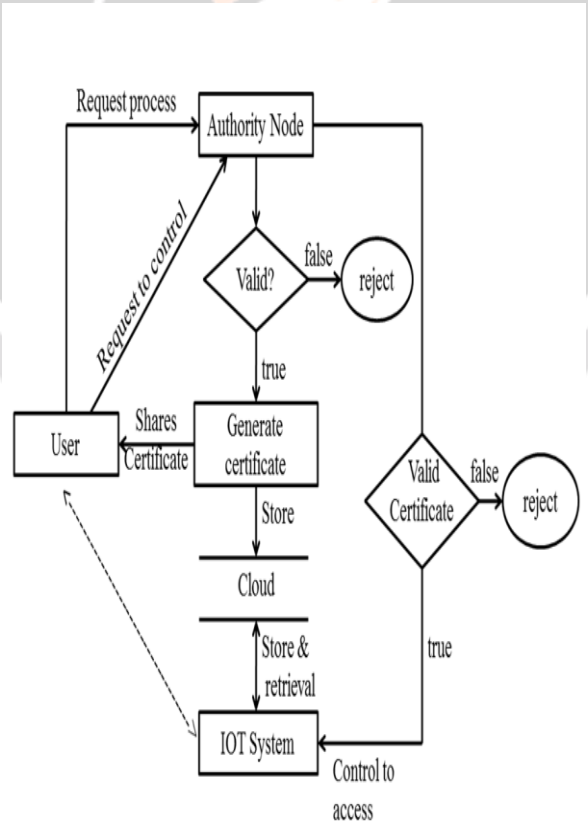

Fig 1. Secured authentication architecture

5 PHASES

- Registration: The Registration process is carried out between the recently joined client and the Authority Node.
- Communication: The next process is theprocess of Communicationwheresecure message is used for information transmission.

6 DATABASE

The schema consists of three tables, which are as follow.

1. Requests table
2. Control_Request table
3. Iot_command table

The Request table contains the information about clients such as Request id, Mac id, Ip address, Username Machine name and Certificates & Keys. This table is used in Registration phase. The Control_Request table contains the information about Mac id, Otp, Session key, Timestamp. This table is used in communication phase while clients send requests to cloud for controlling the IoT system. Iot_command table contains session key and the command sent from client. This table is used in communication phase when client is accessing the IoT systems.

7 .ROLES

1. Client: The client machine which wants to gain access to the IoT system must register to the cloud server by sending all information about the client machine like mac id, IP address etc., after authentication client can access IoT system by gaining access permission from cloud server.
2. Cloud Server: Cloud server accepts client request for registration, server maintains all details about client system. Server handles generation of public and private key, certificate to authenticate client and it also take care about granting access to the client to use IoT system by using SHA algorithm.
3. Machine learning: Machine learning supervised algorithm is used to keep track of the clients which has failed to gain access to the IoT system, by maintaining logs if unauthorized client try to access the IoT device access will be denied.

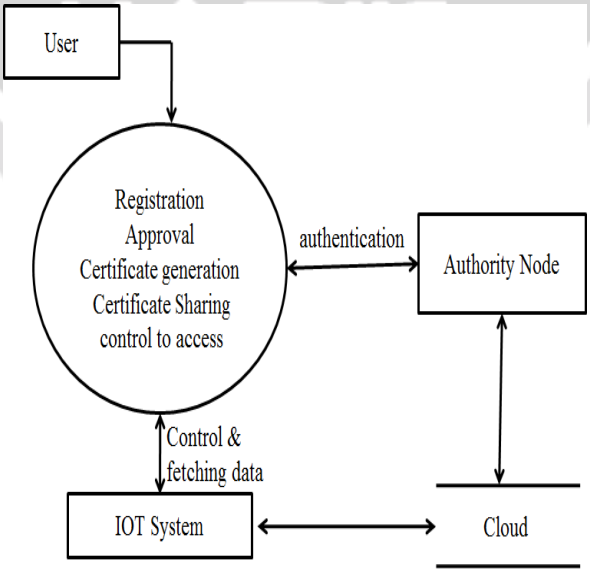

Fig 2. Roles mechanism

8. CONCLUSION

This paper addresses the security problem, by proposing a peer-to-peer security protocol to satisfy the varied environment. Secure communication is implemented on an open sourced platform for the Internet of Things. Security is provided by allowing only authorized user to use the specified IoT system facility, authentication process is conducted for the client machine after client authentication is passed then communication between client and IoT system is permitted.

9 .REFERENCES

[1] IoT Analytics. Why the internet of things is calledinternet of things: Definition, history, disambiguation. https://iot-analytics.com/internet-of-things-definition/.

[2] "Privacy and authentication in the Internet of Things" published inmarch 2015, sourced from Manfred Kube, Gemalto

[3] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan.Internet of things (iot) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Trans-actions (ICITST), pages 336–341, Dec 2015.