Survey on Trust Problem and Provocation in the Internet of Things

G. Manjula[1] A. Bhagyalakshmi[2]
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, India

Abstract— IoT refers to the interconnection of the scattered physical object under a backbone environment. The scope of IoT is not just connecting things (devices, applications, and machine) to the internet. It also allows these things to communicate and exchange data. The survey is about trust problem and challenges in IoT.

Keywords: IoT (Internet of Things), Blockchain, Cloud

I. INTRODUCTION

In the upcoming years, the Iot devices will be a part of the mainstream electronics culture and people will adapt to these smart devices. Expert says that by the year 2020, there will be a total of 50 million devices/things connected to the internet. An Iot device consists of several interfaces for connecting to other devices both wired and wireless they are

1) I/O interfaces for sensors
2) interfaces for Internet Connectivity
3) Memory and Storage Interfaces
4) Audio and Video interfaces

II. LITERATURES

The trust can be achieved by providing Privacy and Security in Iot devices. Iot Security is the subject of scrutiny after a number of high profile incidents where a common Iot device used to infiltrate and attack the larger network. Trust is a different concept and is influenced by many measurable and non-measurable properties[1].Security is ensured by the user safety and system security is the basic to gain trust. In olden days IT security is an add on security with complex Algorithm. But now in Iot, they consist of inbuilt security with a lightweight algorithm for resource-constrained devices[1].

Privacy is ensured how the entity provide authorization, authentication ie when and to whom the information should be shared[1].According to the Iot Indian Market, there will be a huge growth from $15 million with 2.7 billion units from the current $5.6 billion and 200 million connected devices[2].The On-demand Security configuration technique is used easily to set or make a change in any security functionality of a device. In this technique, the security profile and configuration mapping are introduced .The security profile work is gathering and analyzing information without any redundancy. The configuration mapping is used to create and reconfigure the device image for the current time of security configuration. Now the map contains information about present security modulus in the devices and put them according to the map without any recreating device image. Figure 1 shows the on-demand security configuration of the device[3].

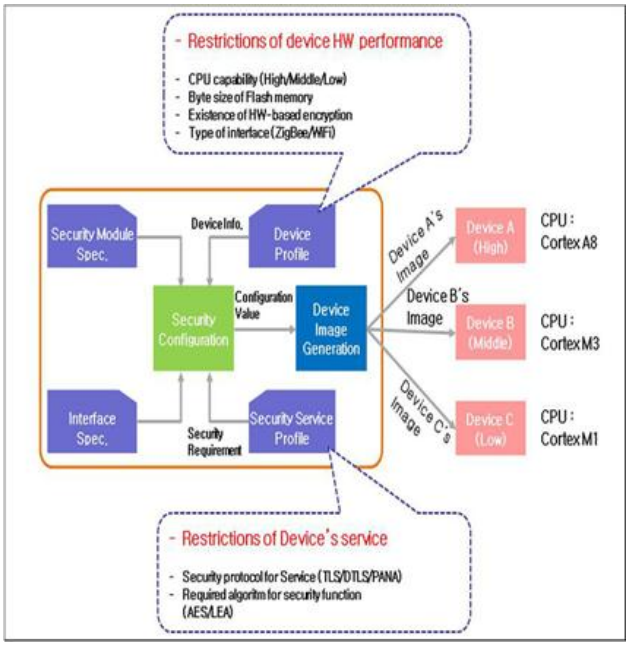

Fig. 1: On-demand security

To ensure security authentication and authorization are important. OAuth 2.0 is a security component is used in oneM2M for security purpose. The security component will provide a token Request and response, unauthorized user request will be blocked. The authorized user request only will be passed on the oneM2M Security component [4]. The OAuth 2.0 General Framework is shown below in figure 2.To provide security and confidentiality of the shared information here is a method called Information management procedure based on the reference model of Iot [5].The system consists of 3 phases.

1) Information Gathering
2) Information Verification and Analysis
3) Information Sharing

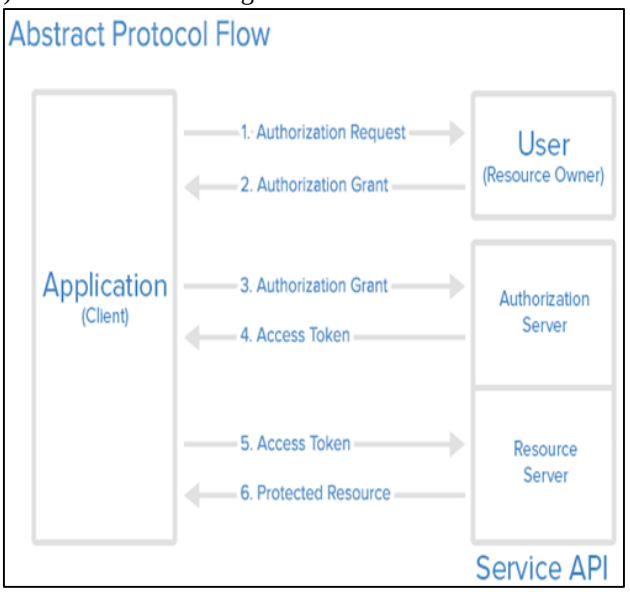

Fig. 2: OAuth 2.0 General Framework

To secure Iot devices here is a solution for 2 threats are Device Cloning attacks and Sensitive data exposure. Many devices send their data to the third party (Cloud) that wouldn't do any identity checking and that allows attackers to create clones leads to the problem such as first identify the authorized devices to prevent malicious clones to be registered with the system and upload vulnerable data .we could able to prevent a user to know about the current traffic while transmitting sensitive data by Iot devices. The solution for the problem is the clone attacks can be identified in milliseconds and the size of the data should not increase 8-byte postencryption. This solution works on low powered hardware and the working times and size of data wouldn't grow exponentially [6].To improve security and safety in Iot device a server is introduced known as Remote Security Management Server[RSMS].The RSMS provide function such as Confidentiality, integrity, authorization, authentication. There are 16 security function modules with a repository database it has information about security management. Every module has a unique security function. If a hacker attack, this method will help us in reducing damage by a quick and effective solution through device monitoring, intrusion detection [7]. Blockchain is simply a ledger maintained by an Organisation. The blockchain is mostly used in the finance area i.e A well-known cryptocurrency Bitcoin. To provide security for iot system blockchain network is used. Blockchain consists of two fields:

1) by generating decentralized system
2) transperent database

A. Pillars of Blockchain:

1) Consensus: proof of work (PoW) and verifies the transaction in the network.
2) Ledger: Complete data about transaction within the network.
3) Cryptography: Ensures all data in the ledger and network get encrypted and only authorized user can decrypt the information.
4) Smart Contract: Verify and Validate the users of the network.

The blockchain is implemented by 3 domains:

1) Public: Open-Area, All nodes can read or write transaction that is taking part in the consensus process without any permission required. In this category, Bitcoin and Ethereum will come.
2) Consortium Area: Here partial permission will take place only known nodes will take part in the consensus process, here the permission to read or write may be public or only a few authorized nodes.
3) Private: It is the restricted area, only the organization which it has given rights to modify to whom the network of blockchain belongs to. Reading of transaction may or may not be public. It is mostly deployed in industries. The figure 3 shows the pillars of the blockchain[8].

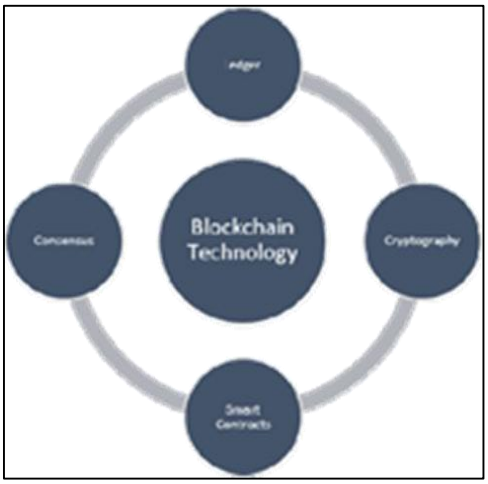

Fig. 3: Pillars of Blockchain

In Blockchain, General Database will be used, but here they introduced an Ethereum database i.e virtual currency which is from the existing bitcoin. The Ethereum support numerous application such as SNS, E-mail, electronic voting, etc.In the existing General Database uses Mysql server has much vulnerability such as SQL injection, now the Open Source Iot Server Platform does not use MySQL.

B. Smart Contract:

It is the first blockchain, that is bitcoin script allow limited information and the bitcoin script won't use a loop so ethereum is used as a solution for loops and used to store real-time sensor data in a block by using smart contract ethereum.[9].One of the features of blockchain technology is democratizing the process of transaction validation and commitment. It results in eliminating the use of trusted centralized ledger. Also, another feature is a smart contract which is supported by all blockchain based network. Smart contract not only allows the users to issue transactions transferring assets between them but also enable them to regulate the financial transactions between them without the need of a trusted third party. In this paper, they proposed an architectural guideline for blockchain enables Iotdevices. Here Ethereum blockchain network is used for the shared resources to connect directly to the blockchain and are controlled by smart contract with the help of the smart contract they receive and update the security parameters and user's information[10].

C. Security Requirements:

Security plays a vital role in every industry. To develop any product security must be added from the initial stage itself. Security is used to treat the root cause of the problem not its symptoms.

D. Confidentiality:

while delivering user's privacy data during the smart home device inter-communication and the key information used for encryption algorithm should be secured properly to prevent any exposure to the outside. To secure transferring the data generated from one device into another device the data must be enclosed with a key and end it be as ciphertext form. To avoid any replication and modification by the middleman and provide a high end secured password setting and periodic password change must be used.

E. Integrity:

To ensure reliability, unauthorized access should be avoided. User's private data and the key information used or encryption should not be forged or tampered. Mutual authentication between devices and reliable communication should be configured. Data integrity should be provided while sending the data generated from the device to another device.

F. Availability:

Immediate response to security threats such as cyber attacks, hacking, etc. Software update must be ensured by periodical monitoring the status of the device and if any abnormal operation is generated from the device should be accompanied.

III. Conclusion

In this paper, we surveyed about internet of things security, privacy, problems and challenges .To ensure trust, security and privacy plays an important role in internet of things. In our future work, we are going to work in vulnerability threats over network and some privacy techniques over the networks.

References

[1] MarioFrustaci, Pasquale Pace, GianlucaAloi, and Giancarlo Fortino. "Evaluating Critical Security Issues of the Iot World: Present and Future Challenges" IEEE Internet Of Things Journal, Vol.5, No.4, August 2018.
[2] Er.PoojaYadav, Er. Ankur Mittal, Dr.HemantYadav IoT: Challenges and Issues in Indian Perspective" 978-1-5090-6785-5/18/$31.00 © 2018 by IEEE.
[3] Boheung Chung, Jeongyeo Kim, and YoungsungJeon "On-demand security configuration for IoT devices" 978-1-5090-1325-8/16/$31.00 ©2016 IEEE.
[4] Se-Ra Oh,Young-Gab Kim, "Development of IoT SecurityComponent for Interoperability"978-1-5386-4266-5/17/$31.00©2017 IEEE.
[5] Jongsoek Choi, Yongtae Shim, Sunok Cho, "Study on Information Security Sharing System among the Industrial IoT Service and Product Provider"978-1-5386-2290-2/18/$31.00 ©2018 IEEE.
[6] SwapnilNaik,VikasMaral,"Cyber Security – IoT"2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.
[7] Seungyong Yoon, Jeongnyeo Kim,"Remote Security Management Server For IoT Devices" 978-1-5090-4032-2/17/$31.00©2107 IEEE.
[8] Madhusudan Singh, Abhiraj Singh, Shiho Kim, "Blockchain: A Game Changer for Securing IoT Data"2017 IEEE.
[9] Jin HyeongJeon, Ki-Hyung Kim, Ki-Hyung Kim, "Blockchain-based data security enhanced IoT Server Platform" 978-1-5386-2290-2/18/$31.00 ©2018 IEEE.
[10] ArmanPouraghily, MdNazmul Islam, SandipKundu, Tilman, Wolf," Poster Abstract: Privacy in Blockchain-Enabled IoT Devices" 2018 IEEE/ACM Third International Conference on Internet-of - Things Design and Implementation
[11] I K Poyner, R S Sherratt, "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people."

