Gateway Supported Security Enhancement in the Internet of Things(IoT)

Sowmya B[1], Dr.Veeragangadhara Swamy T.M[2]

[1]MTECH 4[TH] SEM, Dept. Of Computer Science and Engineering, RYMEC.

[2] PROFESSOR, Dept. Of Computer Science and Engineering, RYMEC.

ABSTRACT

Now a days, the popularity of the Internet of Things (IoT) has led to a very rapid development and significant advancement of ubiquitous applications seamlessly that are integrated within our daily life. Owing to the accompanying growth of the importance of privacy, a great deal of attention has focused on the issues of secure management and robust access control of IoT devices. In this paper, we propose the design of a blockchain connected gateway which adaptively and securely maintains user privacy preferences for IoT devices in the blockchain network. Individual privacy leakage can be prevented because the gateway effectively protects sensitive data from being accessed without their consent. A robust digital signature an encryption mechanism is proposed for the purposes of authentication and secure management of privacy preferences. Furthermore, we adopt the blockchain network as the underlying architecture of data processing and maintenance to resolve privacy disputes.

Keywords: Internet of Things(IoT), Blockchain network, BlockChain Gateway(BC Gateway).

1. INTRODUCTION

Internet of things (IoT) equipped with electronic device are widely trending in this modern era, devices like Passive Radio Frequency (RF) or Blue Tooth Low Energy (BLE) are examples for such devices. These devices are mainly used for the identification purpose and computing for the communication capabilities as well as used as the real world applications. And one kind of example we can see here is the common wearable's with biometric data, retrieval data and health management have become popular in daily life.

Figure 1: Example of User wearable Device

As we can seen in the figure 1 there are wearable devises based on BLE use to monitor the human body conditions like heart beat sensor, intelligent glass, smart shows which are used in tracking status of human body. So, mainly in this technology privacy leakage may occur i.e., the data leakage may happen between

the hardware point are variable itself, are it could happen between wearable device and mobile gateway like the smart phone.

So this study designs and proposes and gateway supported security enhancement in IoT. Here we are using Blockchain Network for the management of privacy preferences. Blockchain technology where mainly focuses on the security i.e., to protect and manage the user preferences that are maintained. So this is all done through an gateway called Blockchain Gateway which intensifies the privacy protection where as the IoT devices are still in need.

2. RELATED WORK

Blockchain gateways is also proposed , where these tailored for use with IoT scenarios for obtaining user consent for IoT applications in the health care domain which are proposed are explained in various papers, In [1,6,7] With rapid growth of IoT applications with threatens effecting users privacy . Soon, users will be surrounded by a significant number of devices bearing sensors. These devices will collect data that can be used to monitor users and create user profiles, with or without their consent. [2,5] IoT objects are equipped with electronics, such as passive Radio Frequency (RF) tags or Bluetooth Low Energy (BLE) modules, to provide the objects themselves with identification, computing, and communication capabilities to support versatile ubiquitous service applications in the real world. [3,4] IoT empowers to connect and communicate and converting the physical world into an enormous information system. Various technologies, like Cloud Computing and Machine Learning to Data Analysis and Information Modeling, are quickly becoming an integral part of IoT fabric. The tremendous advancement in the field of IoT is causing growth in Information and Communication Technology (ICT) business as well.

3. EXISTING SYSTEM

In the existing system although it offers a good privacy solution but there is no guarantee for the leakage of data. Though we need IoT devices to support the operation, and also modifying are replacing these IoT devises may be cost efficient as well. So, to overcome this we have introduce and technology proposed in proposed system.

DISADVANTAGES OF EXISTING SYSTEM:

- Cost Efficient.
- Modifying or Replacing is a tedious job.
- Privacy is not guarantee.

4. PROPOSED SYSTEM

Enhancing the existing system we have proposed a system to overcome the drawbacks of the privacy and security issues that will occur in the present system. So we are proposing a system (BC Gateway) that is Blockchain connected gateway which uses the Blockchain Technology.

Here we are proposed with one modules. Firstly the administration module for connection with the BC gateway. Second one is the when a user connect his/her smart phone to the BC gateway. So it mainly focuses on consistent concentration on BC gateway where it is utilizing the technology of Blockchain for privacy and security purpose and thus Quashing disputes in privacy practices.

ADVANTAGES OF PROPOSED SYSTEM :

- Enhance security
- Privacy is a key factor
- Transactions are not lost they can be retrieved.

5. METHODOLOGY

In general there are three steps of participants involve. They are :

1. The owner or administrators of IoT devises
2. The BC gateway administrators &
3. The end users

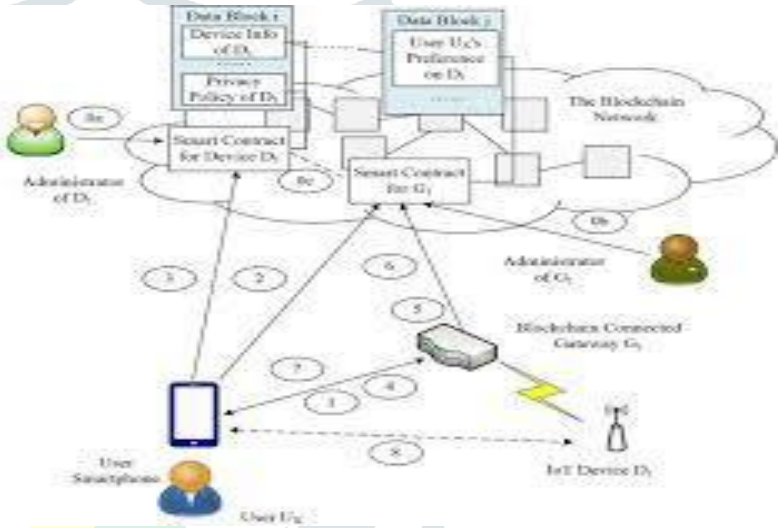

Figure 2: Various operations related to System

In figure 2 the information must be stored first in order to excess the information so this path is done by administrator of the devise. So the information like devise name, manufacture related information, features etc., and also other attributers like privacy policies. Here the administrator can create a smart contract for the gateway administrator which will link the smart of the devise.

Step 1 : User uses the smart phone to connect the BC gateway

Step 2 : User can obtain the address of the gateways smart contract

6. CONCLUSION

This paper contributes and mainly eliminates the disputes arising in the privacy. The BC gateway which we are using acts as are intermediator between IoT devise and users. Hence we are introducing this technology for preventing the sensitive data leakage that is happen between various devices. Thus this can be implemented in many real world applications as it is trust worthy application.

7. FUTURE ENHANCEMENT

As future work, we intend to investigate further the issues that surround each of the components that comprise the proposed framework of data privacy. In addition we can implement step 3 that is the user can retrieve the address of IoT device smart contract and fetch device information and privacy policies ,step 4 user can connect to associated BC gateway and notify the gateway and step 5 storing the preference data in BC gateway step 6 preservance of the data in an BC network step 7 & 8 gateway will process the request made by the user preference and other module we can further enhance one is the when a user connect his/her smart phone to the BC gateway.

Hence we use this technology called Block chain which is connected via BC gateway to protect the user preference and privacy.

9. REFERENCES

[1] Konstantinos Rantos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis3 and Alexandros Papanikolaou Block chain-based Consents Management for Personal Data Processing in the IoT Ecosystem ISBN: 978-989-758-319-3 Copyright © 2018 by SCITEPRESS – Science and Technology Publications pp.211-220.

[2] SHI-CHO CHA, JYUN-FU CHEN, CHUNHUA SU, AND KUO-HUI YEH, A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things Received November 28, 2017, accepted January 21, 2018, date of publication January 30, 2018, date of current version May 24, 2018., Digital Object Identifier 10.1109/ACCESS.2018. 2799942 pp. 236-248.

[3] Alfonso Panarello , Nachiket Tapas , Giovanni Merlino, Francesco Longo and Antonio Puliafito Blockchain and IoT Integration: A Systematic Survey Received: 26 June 2018; Accepted: 2 August 2018; Published:6 August 2018, Sensors 2018, 18, 2575; doi:10.3390/s18082575 pp. 117-130.

[4] Castro, M.; Liskov, B. Practical byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 1999), New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.

[5] EU Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, European Commission, Brussels, Belgium, 2014.

[6] Bartolini, C., Muthuri, R., and Santos, C. (2017). Using ontologies to model data protection requirements in workflows. In New Frontiers in Artificial Intelligence, volume 10091, pages 233–248. Springer.

[7] Buterin, V. (n.d.). A next-generation smart contract and decentralized application platform. Available online at: https://github.com/ethereum/wiki/ wiki/White-Paper.