International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842
Issue 06, Volume 6 (June 2019) www.irjcs.com
SPECIAL ISSUE - 5th International Conference - "ACCE – 2019"

BLOCKCHAIN FOR FINANCIAL APPLICATION USING IOT

Aruna Reddy H, Kavya Raveendra Bhat , Pavithra M, Mandara N, Ramya S
Dept. of Information Science,
Vemana Institute of Technology (Affiliated to VTU), Bangalore, India
arunahreddy@gmail.com; kavyaryalavalli@gmail.com; pavithrashetty3698@gmail.com;
mandaransharma@gmail.com; ramyagowda1108@gmail.com

Manuscript History
Number: IRJCS/RS/Vol.06/Issue06/JNCS10136
Received: 29, May 2019
Final Correction: 30, May 2019
Final Accepted: 02, June 2019
Published: June 2019
doi://10.26562/IRJCS.2019.JNCS10136
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract - Recently, the popularity of the Internet of Things has led to a rapid development and significant advancement of ubiquitous applications seamlessly 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. The design of a blockchain connected gateway which adaptively and securely maintains user privacy preferences for IoT devices in the blockchain network also individual privacy leakage can be prevented. A robust digital signature mechanism is proposed for the purposes of authentication and secure management of privacy preferences. A secured payment is done using the gateways. Blockchain network is adopted as the underlying architecture of data processing and maintenance to resolve privacy disputes. Here we are using the blockchain to store sensor details, user information, and payment details for user transactions.

Keywords – Blockchain, Internet of Things, Privacy, Security.

I. INTRODUCTION

The blockchain for financial application is very important solution to improve privacy of the data. Earlier the sensor data stored in the accessed data via cloud. There are much chances that the service provider may change the data to make profit to some organization and because of that user may not receive correct data. Here the motivation is to protect data privacy and maintain transparency. Thus blockchain network is used as the underlying architecture for management of privacy preferences. That is, the proposed Blockchain Connected gateway uses blockchain technology to protect and manage the maintained user preferences from being tampered with. Therefore, the BC gateway enhances user privacy protection while legacy IoT devices are in use. In addition, the blockchain base user preferences management scheme is useful for solving disputes between user and IoT applications Providers when it comes to privacy practices.

II. ARCHITECTURE OF PROPOSED SYSTEM

In general there are three main participants are involved in the proposed system. (1) the owner of IoT devices (2) the BC gateway (3) the end users. Here we demonstrate an overview of the functionalities of proposed BC gateway as shown in Fig 1. The IoT device administrator will create a smart contract for the device and use this contract to manage device's information (device name, device type, features and so on) and privacy policies of the devices (step 0a). The blockchain gateway (BC gateway) administrator can also create a smart contract for the gateway (step 0b). After the gateway connected with the IoT device physically, the BC gateway administrator will link the smart contract of the device to the smart contract of the gateway. When a user uses his/her smartphone to connect with BC gateway (step 1), user will obtain the address of gateway's smart contract. User can query the list of devices connected to the gateway from the gateway's smart contract (step 2).

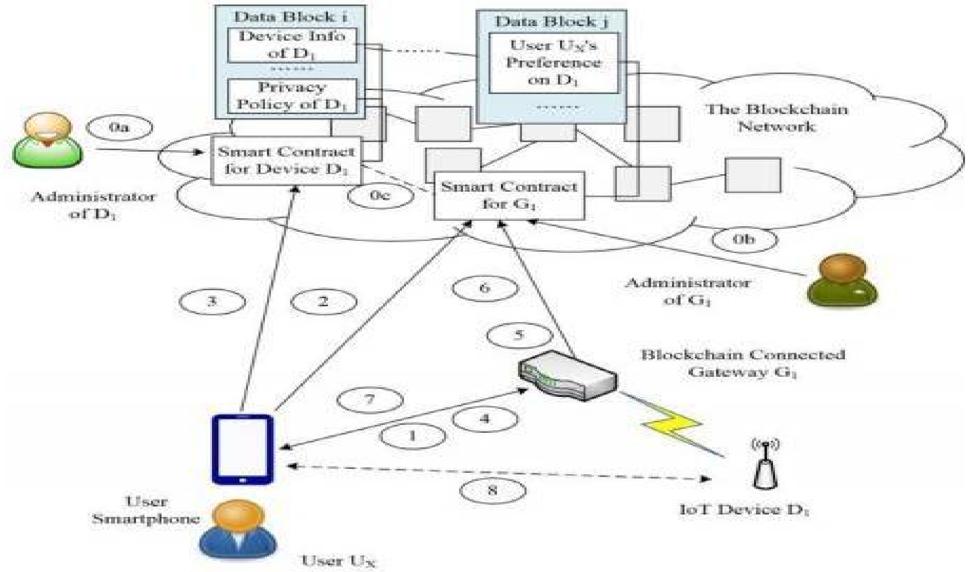


Figure 1: Architecture of proposed system

Then the user can retrieve the address of an IoT device's smart contract and fetch the device information and privacy policies via smart contract. After seeing the privacy policies of an IoT devices, a user can accepts or decline the policies (step 4) by connecting with the BC gateway. The data will be stored in gateway (step 5) which in turn stored in blockchain (step 6). When the user access the IoT device via gateway (step 7 and step 8), the gateway will process user requests based on the preserved user preferences.

III. ALGORITHM

Here we are using Digital Signature Algorithm (DSA) to establish this architecture. The DSA algorithm works in the framework of public-key cryptosystems and is based on the algebraic properties of the modular exponentiations, together with the discrete logarithm problem. Messages are signed by the signer's private key and the signatures are verified by the signer's corresponding public key. The digital signature provides message authentication, integrity and non-repudiation.
DSA parameters:

- P = a prime modules, where $2^{L-1} < p < 2^{L}$ for $512 \le L \le 1024$ and L is a multiple of 64. So L will be one member of the set {512, 576, 640, 704, 768, 832, 896, 960, 1024}
- q = a prime divisor of p-1, where $2^{159} < q < 2^{160}$
- $g = h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < p - 1$ such that $h^{(p-1)/q} \bmod p > 1$ (g has order q mod p)
- x = a randomly or pseudo randomly generated integer with $0 < x < q$
- $y = g^{x} \bmod p$
- k = a randomly or pseudo randomly generated integer with $0 < k < q$

Generation of Prime p and q
The generation is hard to understand but I found a good description of it…

The prime generation scheme starts by using the SHA and a user supplied SEED to construct a prime, q, in the range 2159 < q < 2160 . Once this is accomplished, the same SEED value is used to construct an X in the range 2L-1 < X < 2L . The prime, p, is then formed by rounding X to a number congruent to 1 mod 2q as described below. An integer x in the range 0 ≤ x < 2 g may be converted to a g-long sequence of bits by using its binary expansion as shown below:
x = x1* 2g-1 + x2* 2g-2 + ... + xg-1* 2 + xg -> { x1,..., xg }.
Conversely, a g-long sequence of bits { x1,..., xg } is converted to an integer by the rule
{ x1,..., xg } -> x1* 2g-1 + x2* 2g-2 + ... + xg-1* 2 + xg.
Note that the first bit of a sequence corresponds to the most significant bit of the corresponding integer and the last bit to the least significant bit.

Let L -1 = n* 160 + b, where both b and n are integers and 0 ≤ b < 160.
Step 1. Choose an arbitrary sequence of at least 160 bits and call it SEED. Let g be the length of SEED in bits.
Step 2. Compute U = SHA-1[SEED] XOR SHA-1[(SEED+ 1) mod 2 g].

Step 3. Form q from U by setting the most significant bit (the 2159 bit) and the least significant bit to 1. In terms of Boolean operations, q = U OR 2159 OR 1. Note that 2159 < q < 2160.
Step 4. Use a robust primality testing algorithm to test whether q is prime 1.
Step 5. If q is not prime, go to step 1.
Step 6. Let counter = 0 and offset = 2.
Step 7. For k = 0,..., n let Vk = SHA-1[(SEED + offset + k) mod 2g]. 1 A robust primality test is one where the probability of a non-prime number passing the test is at most 2-80
Step 8. Let W be the integer W = V0 + V1* 2160 + ... + Vn-1* 2(n-1)* 160 + (Vn mod 2b) * 2n* 160 and let X = W + 2L-1 . Note that 0 ≤ W < 2L-1 and hence 2L-1 ≤ X < 2L.
Step 9. Let c = X mod 2q and set p = X -(c -1). Note that p is congruent to 1 mod 2q.
Step 10. If p < 2L-1 , then go to step 13.
Step 11. Perform a robust primality test on p.
Step 12. If p passes the test performed in step 11, go to step 15.
Step 13. Let counter = counter + 1 and offset = offset + n +1
Step 14. If counter ≥ 212 = 4096 go to step 1, otherwise (i. e. if counter < 4096) go to step 7.
Step 15. Save the value of SEED and the value of counter for use in certifying the proper generation of p and q.

IV. MODULES

There are four modules in the proposed architecture namely (1) Service Provider (2) IoT devices (3) User service mapping (4) Accessing data.

1. Service Provider

The service provider can register in the portal. While registration the service provider needs to provide the company details such as company name, contact number and the list of services provided by them. While adding the services service provider provides the name of the services, devices used to provide the services the device manufacturer details and version of the devices; along with the service cost details are provided. The services cost has three categories like daily, weekly and monthly basis services. The security features for doors services need to be provided by the service provider. This detail includes the level of security privacy policies reliability etc. All these details are stored in the blockchain gateways.

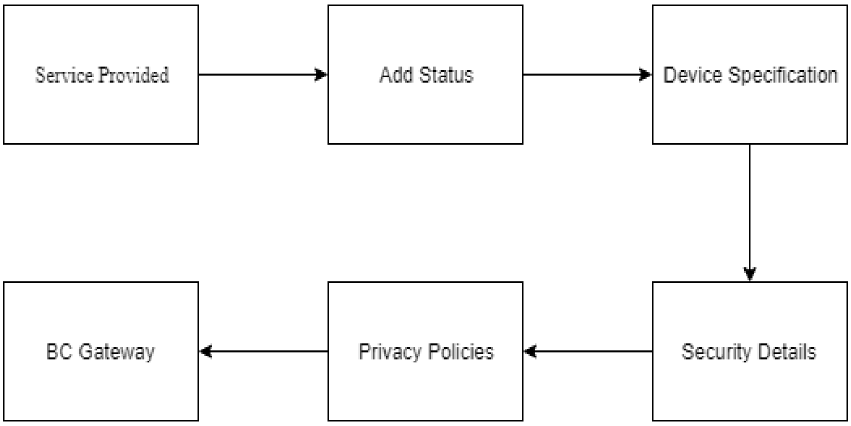


Figure 2: Service provider

2. IoT device

The services that all provided by the service provider includes IoT sensors that are connected with the IoT network. The sensor devices are Temperature sensor (LM35), Digital Humidity Temperature sensor (DHT11), Dust sensor (PM 2.5), MQ9 sensor, MQ135 sensor. All these sensors are connected with node MCU separately by it service provider. And these node MCU is connected with the Wi-Fi module. The sensor collected data are passed to BC gateway by gateway administrator and which will be stored in the blockchain.

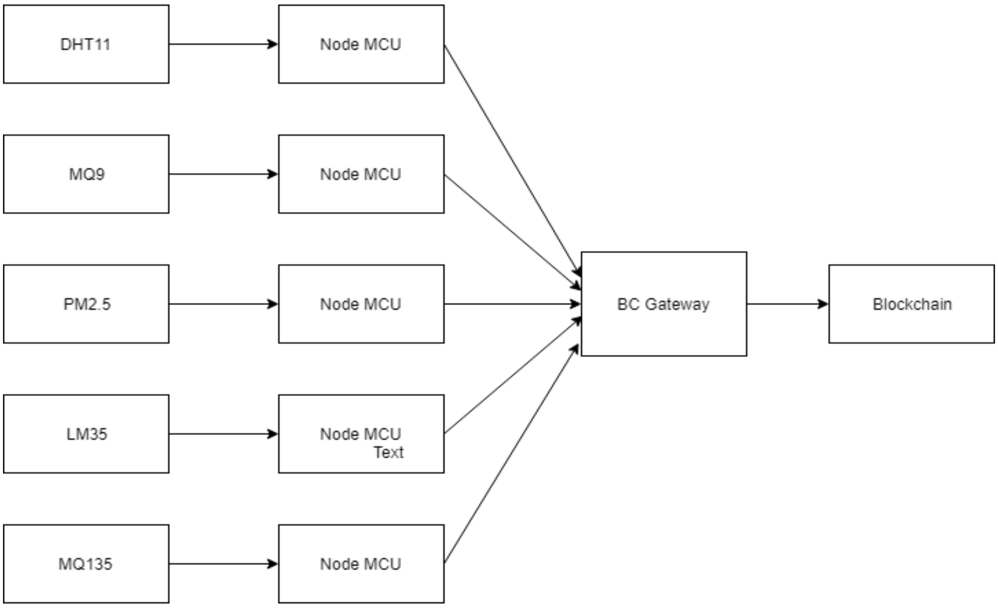


Figure 3: IoT device

3. Service Mapping

User of the Smart City IoT based system can register themselves form the Android based application and this details as store in the server. The user can check the available services by the service provider and can provide their preferences. Based on the user's requirement the BC Gateway maps the privacy policies of the user with available security privacy and policies of the service provider. The BC gateway takes care of the service level agreement of the users as well as also service provider.

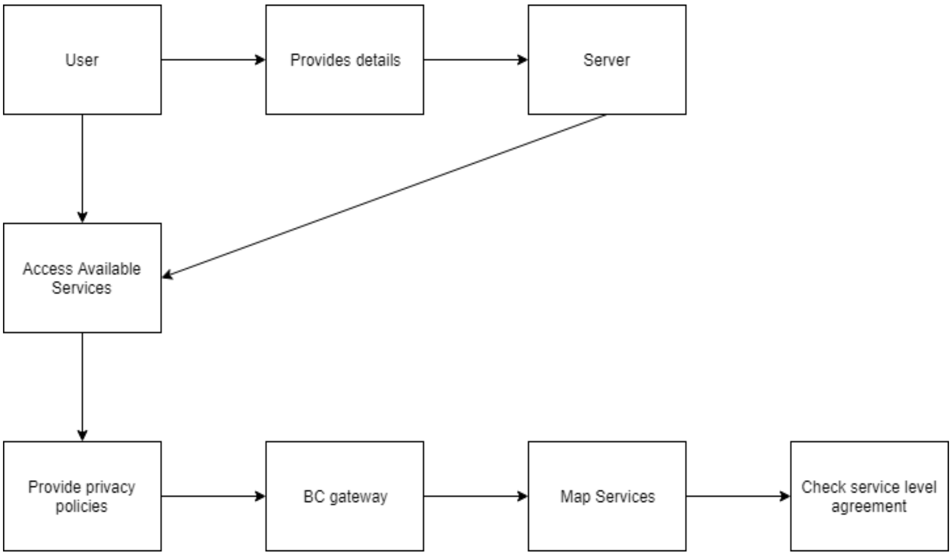


Figure 4: Service Mapping

4. Accessing data

The sensor collected data are stored in the blockchain. Once the data pack show the basic gateway the data with the lame-stamp a stored or added to the chat chain network. When the user BC gateway needs to collect the data, the blockchains collects and send it to user. As the data is in enacted format nodes to decrypt by the BC gateway to serve to the user.

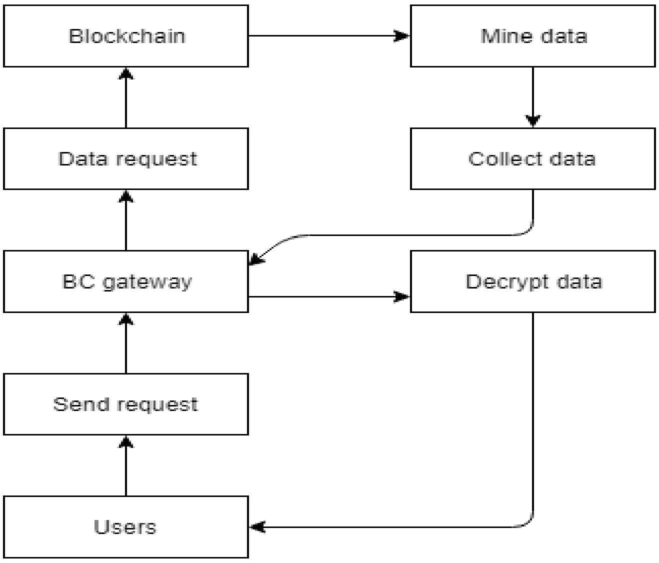
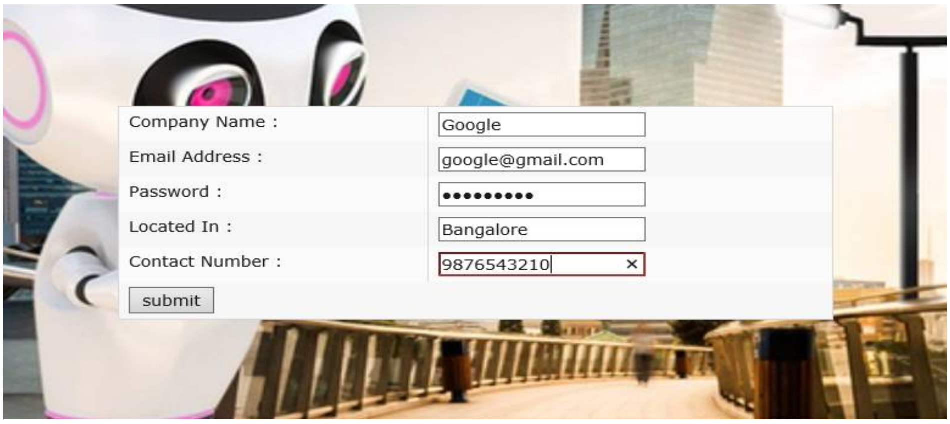


Figure 5: Accessing the data

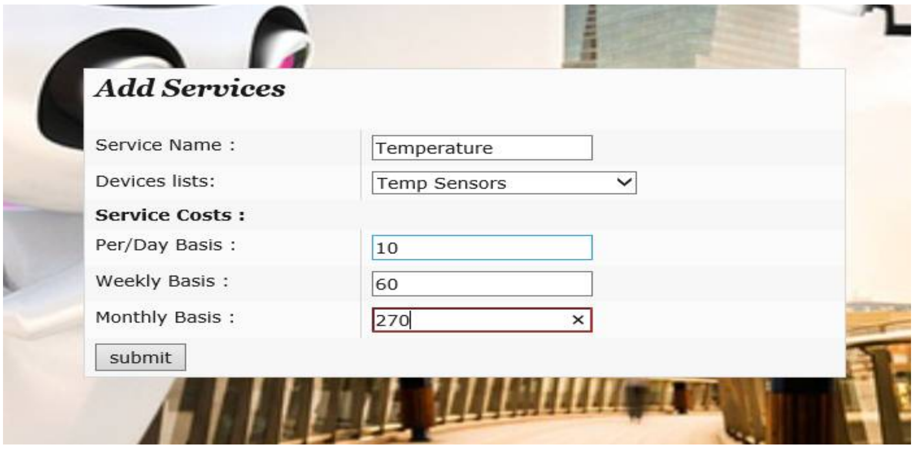
V. RESULTS

The results of the proposed architecture is as follows.



Company Name :	Google
Email Address :	google@gmail.com
Password :	●●●●●●●●●
Located In :	Bangalore
Contact Number :	9876543210

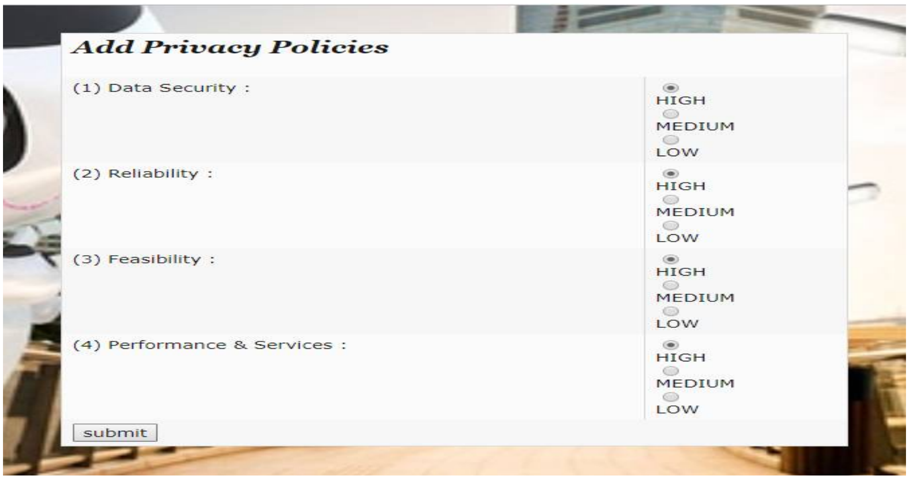
Figure 6: Service provider registration



Add Services

Service Name :	Temperature
Devices lists:	Temp Sensors
Service Costs :	
Per/Day Basis :	10
Weekly Basis :	60
Monthly Basis :	270

Figure 7: Service provider adding services



Add Privacy Policies

(1) Data Security : ● HIGH ○ MEDIUM ○ LOW

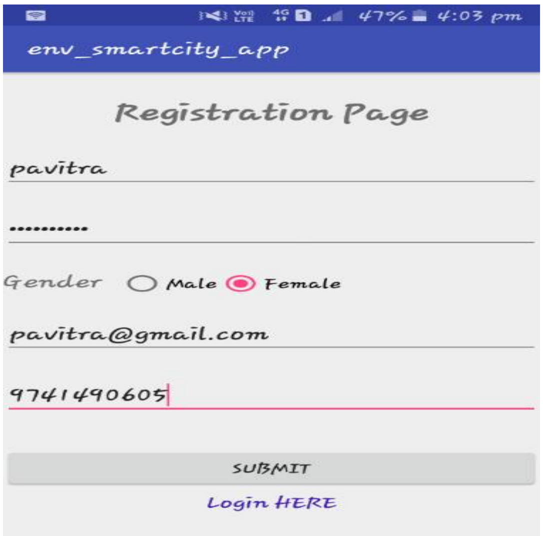
(2) Reliability : ● HIGH ○ MEDIUM ○ LOW

(3) Feasibility : ● HIGH ○ MEDIUM ○ LOW

(4) Performance & Services : ● HIGH ○ MEDIUM ○ LOW

submit

Figure 8: Service provider adding privacy policies



47% 4:03 pm

env_smartcity_app

Registration Page

pavitra

••••••••••

Gender ○ Male ● Female

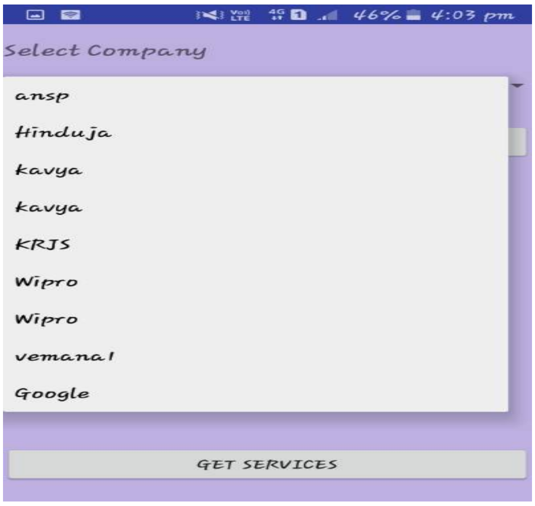
pavitra@gmail.com

9741490605

SUBMIT

Login HERE

Figure 9: User registration using android application



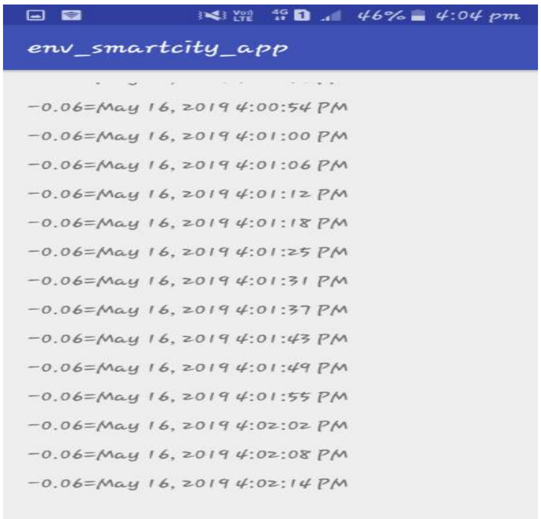
46% 4:03 pm

Select Company

ansp
Hinduja
kavya
kavya
KRJS
Wipro
Wipro
vemana!
Google

GET SERVICES

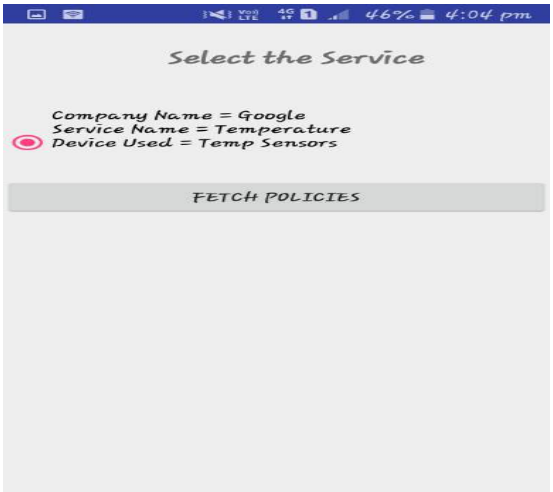
Figure 10: List of companies



env_smartcity_app

```
−0.06=May 16, 2019 4:00:54 PM
−0.06=May 16, 2019 4:01:00 PM
−0.06=May 16, 2019 4:01:06 PM
−0.06=May 16, 2019 4:01:12 PM
−0.06=May 16, 2019 4:01:18 PM
−0.06=May 16, 2019 4:01:25 PM
−0.06=May 16, 2019 4:01:31 PM
−0.06=May 16, 2019 4:01:37 PM
−0.06=May 16, 2019 4:01:43 PM
−0.06=May 16, 2019 4:01:49 PM
−0.06=May 16, 2019 4:01:55 PM
−0.06=May 16, 2019 4:02:02 PM
−0.06=May 16, 2019 4:02:08 PM
−0.06=May 16, 2019 4:02:14 PM
```

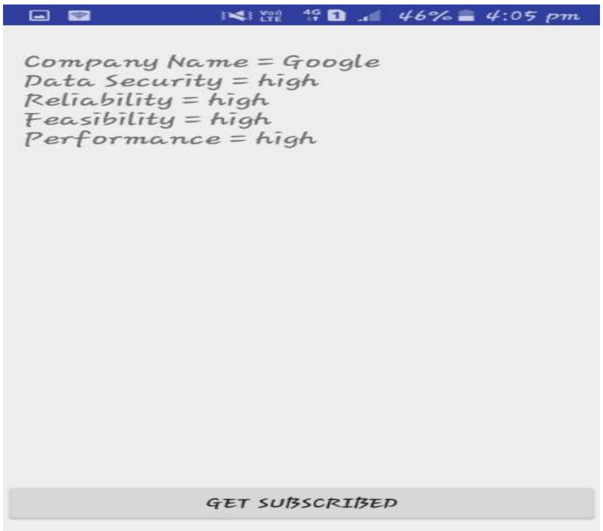
Figure 11: Getting data



Select the Service

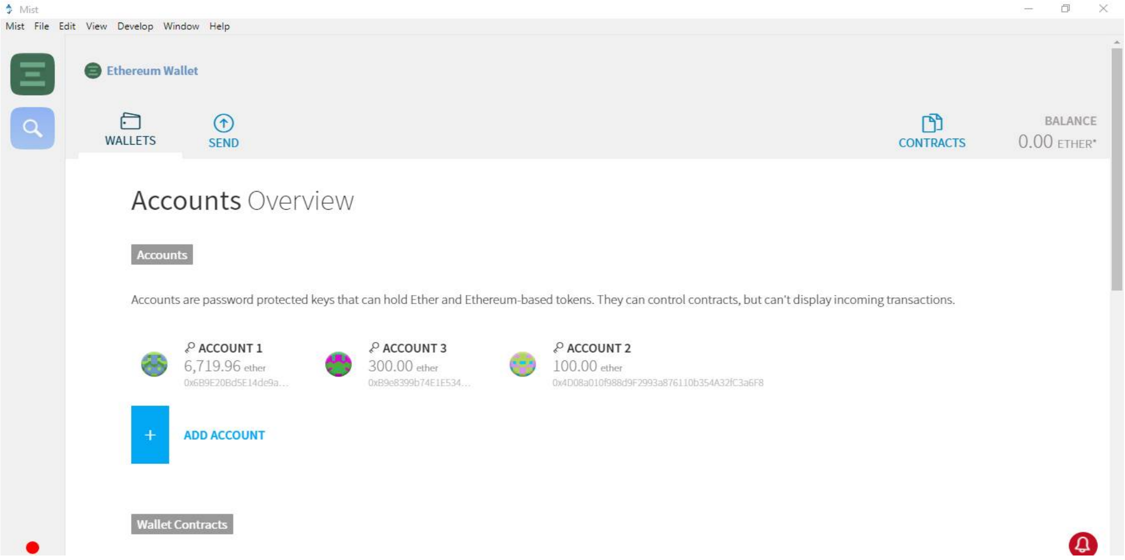
● Company Name = Google
Service Name = Temperature
Device Used = Temp Sensors

Figure 12: Selecting the service



Company Name = Google
Data Security = high
Reliability = high
Feasibility = high
Performance = high

Figure 13: Fetching the privacy policies



Accounts Overview

Accounts

Accounts are password protected keys that can hold Ether and Ethereum-based tokens. They can control contracts, but can't display incoming transactions.

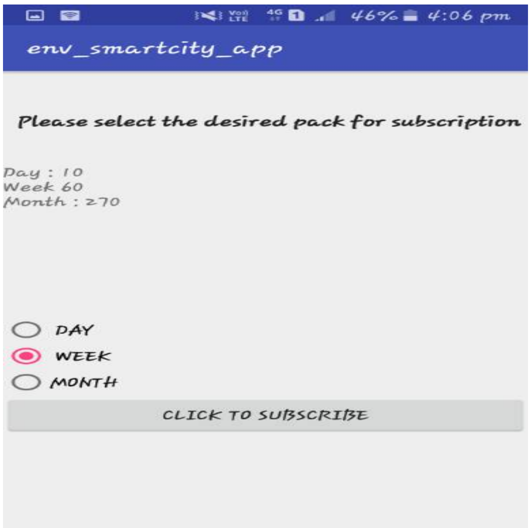
ACCOUNT 1
6,719.96 ether
0x6B9E20Bd5E14de9a…

ACCOUNT 3
300.00 ether
0xB9e8399b74E1E534…

ACCOUNT 2
100.00 ether
0x4D08a010f988d9F2993a876110b354A32fC3a6F8

Wallet Contracts

Figure 14: Balance in the account before subscribing



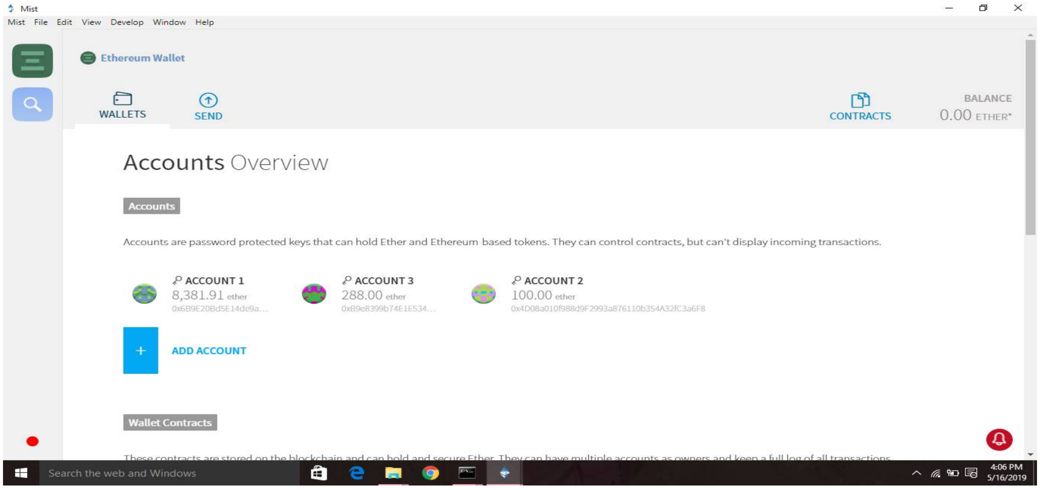
env_smartcity_app

Please select the desired pack for subscription

Day : 10
Week 60
Month : 270

○ DAY
● WEEK
○ MONTH

Figure 15: subscribing to the service



Accounts Overview

Accounts

Accounts are password protected keys that can hold Ether and Ethereum based tokens. They can control contracts, but can't display incoming transactions.

ACCOUNT 1
8,381.91 ether
0x6B9E20Bd5E14de9a…

ACCOUNT 3
288.00 ether
0xB9e8399b74E1E534…

ACCOUNT 2
100.00 ether
0x4D08a010f988d9F2993a876110b354A32fC3a6F8

Wallet Contracts

These contracts are stored on the blockchain and can hold and secure Ether. They can have multiple accounts as owners and keep a full log of all transactions.

Figure 16: Balance in the account after subscribing

CONCLUSION

To enable IoT service providers to obtain user consent on privacy policies without modifying (or replacing) legacy IoT devices immediately, this study has proposed the Blockchain Connected Gateway. The BC gateway plays the role of a mediator between users and IoT devices: users can obtain the device information and privacy policies of an IoT device connected to a BC gateway and access the device via the BC gateway rather than accessing the device directly. Therefore, the BC gateway can prevent the device from obtaining sensitive personal data unless users accept the privacy policies of the device. Moreover, the BC gateway will store a user's preference regarding privacy policies in the blockchain network. Because data stored in the blockchain network are tamper resistant, user preference data stored in the blockchain network can be utilized to resolve disputes between users and IoT service providers. Therefore, this paper can contribute to improving user privacy and trust in IoT applications while legacy IoT devices are still in use.

REFERENCE

1. Security and Privacy Issues for an IoT based Smart Home - Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino Gary Steri, and Gianmarco Baldini.
2. PISCES: A Framework for Privacy by Design in IoT - Noria Foukia, David Billard, Eduardo Solana.
3. Privacy Mediators: Helping IoT Cross the Chasm - Nigel Davies, Nina Taft, Mahadev Satyanarayana, Search Clinch, Brandon Amos.
4. Negotiation based Privacy Preservation Scheme in Internet of Things Platform – Arijit Ukil, Soma Bandyopadhyay, Joel Joseph, Vijayanand Banahatti, Sachin Lodha.
5. A User Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices – Shi Cho Cha, Ming Shiung Chuang, Kuo Hui Yeh, Zi Jia Huang, Chunhua Su.
6. How the Blockchain Revolution Will Reshape the Consumer Electronics Industry – Jong Hyouk Lee, Marc Pilkington.
7. Ethereum: A Secure Decentralised Generalised Transaction Ledger – Dr. Gavin Wood
8. A Digital Signature Based On a Conventional Encryption Function – Ralph C Merkle
9. Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults – Allen Clement, Edmund Wong, Lorenzo Alvisi, Mike Dahlin
10. Architecture of the Hyperledger Blockchain Fabric – Christian Cachin