SECURE ROAMING SERVICES FOR INTERNET OF THINGS ARCHITECTURE

D.Vinu kiruthika [1] , J.C.Kavitha[2]

[1]PG Scholar, CSE Dept., Meenakshi college of Engineering, Chennai, Tamilnadu, India

[2] Faculty of computer science engg, Meenakshi college of Engineering, Chennai, Tamilnadu, India

kiruthika_vinu@yahoo.co.in

Abstract- Internet of things (IoT) is an emerging future networking paradigm. In IoT Communication between heterogeneous networks is very attractive. However ensuring secure roaming service among heterogeneous networks is challenging, since each network will have its own security policies that is different from one another it becomes difficult to fulfil the security requirements from heterogeneous networks and since the processing power of most wireless devices could be limited, hence in such a resource constrained environment there is a need for an encryption technique that should support the low processing speed and limited memory space. The proposed system focuses on providing a universal secure roaming architecture and multi-level privacy preservation. Security is achieved by encryption of data using elliptic curve cryptography which is lightweight, scalable and secure. A conditional privacy-preserving authentication with access linkability aims to provide privacy preservation.

Key words: Elliptic curve cryptography, Anonymous user linkability, authentication, Internet of Things (IoT), privacy preservation, security.

I.INTRODUCTION

Internet of things is an emerging networking paradigm. Internet of things is the network of the things or objects that are encapsulated with the sensors, software and connectivity to exchange data with the connected devices to achieve its service. Each thing is uniquely identified by the computing system that are embedded within. It helps to improve our daily life based on sensors and smart objects working together. In Internet of Things (IoT), everything in the real world becomes virtual, which means that each person and thing will have a readable counterpart on the internet. The virtual entities will produce and consume services and collaborate towards a common goal In IoT Communication between heterogeneous networks is very attractive. However ensuring secure roaming service among heterogeneous networks is challenging. Since most of the solutions are developed to cater to a specific application, there is a rising need for a single platform to provide standard, secure transmission of data. This project aims at defining a single standard security framework.

II RELATED WORK

Chengzhe Lai, Hui Li, Xiaohui Liang, RongxingLu, Kuan Zhang, and Xuemin Shen [1] proposed the need for secure roaming service and multilevel privacy-preservation in mobile subscribers. Any secure roaming scheme is dedicated for only one type of network and it cannot fulfil the security requirements from the heterogeneous networks. A conditional privacy-preserving authentication with access linkability for roaming service aims at providing a universal secure roaming service. In heterogeneous networks, user privacy preservation is an important and challenging issue. In this privacy preservation equates with anonymity, i.e., hiding user's identity. For the purpose of dynamic membership CPAL provides an efficient revocation function. This scheme provide a secure roaming architecture to achieve security and a multilevel privacy preservation technique which is achieved through three levels that includes authentication, anonymity, and anonymous user linking.

Daojing He, Jiajun Bu, Sammy Chan, Chun Chen and Mingjian [2] proposed the need for protocol for wireless communications. People can get connected without any interruption using their devices despite of geographical coverage. A roaming service should be deployed for the seamless connection of the devices. Since the geographical coverage is not limited to home networks ensuring security of mobile users is challenging. In order to preserve privacy a protocol named "PRIAUTH" is proposed. Strong user anonymity is achieved through Priauth. This scheme can sustain against snooping. It provides an effective approach to tackle the problem of user revocation with strong user untraceability. Priauth scheme satisfies the following Server authentication, Subscription validation, Provision of user revocation mechanism, User anonymity and traceability. This protocol involves only the user and the visiting server in each run where the home centre remains untouched thus DoS attack on home centres are prevented.

Yixin Jiang, Chuang Lin, Xumein Shen, Minghui Shi, proposed [3] the need for mutual authentication and key exchange protocols. There are two protocols one for mutual authentication and the other for key exchange with the identity anonymity and one-time session renewal has been proposed. User privacy is achieved through identity anonymity and in-order to mitigate the risk of using compromised session key, the key is renewed frequently. The computation complexity remains same as the existing protocols, whereas the security of the users is improved.

Liang Zhou, Han-Chieh Chao, [4] proposed the need for media aware traffic security architecture for internet of things. Internet of things is an emerging future networking paradigm. It helps to improve and optimize our daily life based on sensors and smart objects working together. The multimedia traffic over the IoT can be classified into: communication, computation, and service. Communication in IoT implies the access of information about an object in the network anytime and anywhere. Computation traffic is processed by mobile agents. Service traffic is measured through score and form. Score indicates the percentage of interest users have in multimedia traffic. Form denotes the content features on each Device.

Rodrigo Roman, Pablo Najera, and Javier Lopez [5] proposed the research paper on securing the Internet of Things. Internet of things is the network of the things or objects that are encapsulated with the sensors and connectivity to exchange data with the connected devices to achieve its service. Each thing is uniquely identified by the computing system that are embedded within. Internet users are already undergoing ceaseless attacks and the growing economy is well-supplied with business model that weakens the internet's ethical use which indicates that this cannot bode well for IoT that incorporates many constrained devices. The challenge is to prevent or at least mitigate the impact of such business models. With the lack of strong security foundations attacks and malfunctions will outweigh the benefits of IoT. A proper technical framework is essential. Every security mechanism must consider

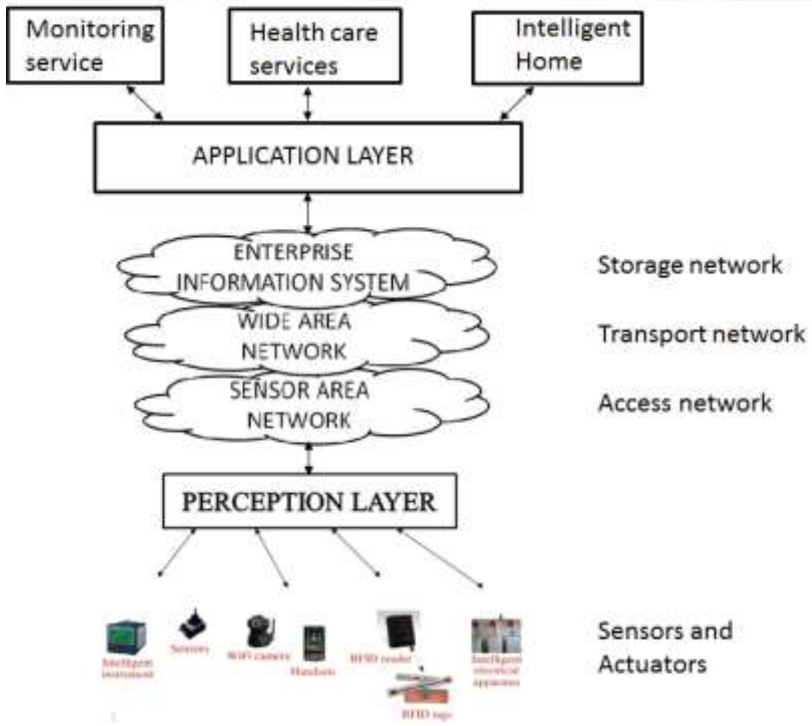
III. EXISTING SYSTEM

The existing system is characterized by three layers sensing layer, network layer, and application layer. The sensing layer is used for collection of the information about an object or a thing in the IoT through sensors. Next it communicates the data through network layer using wired or wireless network. And finally in the application layer it crunches i.e. analyze the data to understand what is happening now and what's likely to happen next. There is a lack of standard secure roaming services in the existing system.

IV. PROPOSED SYSTEM

In the proposed system CPAL scheme is introduced among different networks in IoT to provide a universal secure roaming service. CPAL (A conditional privacy preserving authentication with access linkability) provides privacy preservation in three levels by authentication, anonymity and anonymous authorized user linking. It achieves privacy preservation by hiding the user identity. There is home centre and the visiting centre and the user identity is known only to the home centre this is achieved by a novel group signature technique which effectively mask the user identity. And the security of data is achieved through a lightweight public cryptosystem.

V. SYSTEM ARCHITECTURE



A. System initialization

The process of system initialization includes registering the devices with the network. Once the devices are registered, each device will be uniquely identified using the MAC address or the unique identification provided by the RFID tags. Then the devices can communicate with each other through the network.

The mobile users and the home centre agrees upon with the common parameters before the registration process begin. For registering with the network the following steps are to be performed

A. The mobile users generate a signing key and a verification key using the group signature technique.

B. Then the mobile user generates the user public key and the user signs the request with the signing key and sends it to the home centre.

C. Home centre verifies it with the verification key.

D. If it is valid it generates the id and sends it to the user.

E. Then the user also verifies it, if verification is successful then the registration is complete.

B. **Key generation and encryption**

This includes the generation of keys using elliptic curve crypto system. This is an asymmetric cryptosystem that uses public key to encrypt the message and a private key to generate the signature

Two operations performed on it are Point addition, Point multiplication.

Finite Field: It is a field that contains a finite number of elements, called its order (the size of the underlying set). Operations performed on the elements in finite field includes multiplication, addition, subtraction and division (by anything except zero) have been defined. Finite field exists only when the size is a prime power pk.

EC DOMAIN PARAMETERS

- P is a prime number specifying the underlying finite field Fp.
- a is the first coefficient
- b is the second coefficient
- G represents the base point of the group G = {g,[2]g,[3]g,...,[n−1]g,[n]g},In this case, the element g is called a generator of (G,+).
- n is the order of the group.
- h is the element in G.

KEY PAIR GENERATION

Input : Domain parameters.

Output: Key pair (d, p).

Operation: d = RNG ({1, 2 … n-1}), p = [d] G. Where d is the public key. P is the private key.

Discrete logarithmic problem: Given G and K (G) the attacker would find really hard to find out the k.K is the integer that belongs to G.

Encryption

In order to protect the data that are communicated through the IoT network encryption is needed. The algorithm used here is ECC. Private Key, and public keys are generated for the corresponding user. And since it is asymmetric encryption user’s public key is used to encrypt the message and the private key is used to generate the digital signature. And the receiver’s private key is used to decrypt the message, public key is used to verify the digital signature.

C. User tracking Algorithm

Internet of things is about accessing the information about a particular thing in the internet anytime and anywhere, which leads to a need for proper roaming scheme that would keep track of the user in order to preserve privacy, for a proper privacy preservation there is a need for the architecture that would keep track of the user, in case of any difference of opinion occurs in an access request during roaming, we should equip an algorithm to track the corresponding user of that particular disputed access request message. The detailed steps of the algorithm are as follows.

Step 1) The Home centre retrieves the corresponding user of the disputed message by using a binary search on the registration list.

Step 2) Home centre generates a proof and then sends the proof along with the disputed user id to the judge.

Step 3) judge verifies if he is an authorized user by doing simple computation, if it hold true then the judge proves that he is an authenticated user and cannot repudiate that from using the services.

VI. CONCLUSION AND FUTUREENHANCEMENT

The privacy preservation is achieved by successfully hiding the user entity during registration by CPAL scheme. The data protection is achieved by the encryption using a part of elliptic curve cryptographic algorithm. And in order to keep track of the user during the dispute CPAL provides the user tracking algorithm that would not only help in keeping track of the user, it is equipped with the facility to verify the user to find it out whether he is an authorized user or not without revealing the user identity to the visiting centre. As a future enhancement whenever the authorized network operators or service providers are in need of user statistics on the usage of services it should be equipped with an algorithm that should provide the statistics. Whenever an illegal or exceptional event occurs it should be equipped with a function that could easily revocate the users from the network in case of compromised secret key.

REFERENCES

[1] Chengzhe Lai, Hui Li, Xiaohui Liang, RongxingLu, Kuan Zhang, and XueminShen “A conditional privacy preserving authentication with access linkability for roaming service”, vol. 32 No.4, February 2014.

[2] Yixin Jiang, Chuang Lin, Xumein Shen, Minghui Shi, “Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks”, vol. 38, pp. 1–20, January 2011.

[3] Rodrigo Roman, Pablo Najera, and Javier Lopez “Securing the Internet of Things” January 2011.

[4] Liang Zhou, Han-Chieh Chao, “Multimedia traffic security architecture for Internet of Things” December 2011.

[5] Daojing He, Jiajun Bu, Sammy Chan, Chun Chen, and Mingjian Yin, “Privacy Preserving Universal Authentication Protocol for Wireless Communications”, December 2011

[6] G.Broll, E. Rukzio, M. Paolucci, M. Wagner, A. Schmidt, and H. Hussmann, “Perci: Pervasive service

interaction with the internet of things", December 2009.

[7] C. Fan, Y. Lin, and R. Hsu, "Complete EAP method: User efficient and forward secure authentication protocol for wireless lans", April -2013.

[8] Rodrigo Roman, Pablo Najera, and Javier Lopez "Security analysis and enhancement of 3GPP authentication and key agreement based on EAP-AKA", 2009.