Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 105-115 EISSN 2392-2192

Identity-based Encryption for device-to-device Security in IOT Environments

S. Mohana[1,a], T. K. S. Lakshmi Priya[2,b]

[1]Department of Computer Science & Engineering, Faculty of Engineering, Avinashilingam University, Coimbatore, India

[2]Department of Printing Technology, Faculty of Engineering, Avinashilingam University, Coimbatore, India

[a,b]E-mail address: smohana024@gmail.com , tkslp.dr@gmail.com

ABSTRACT

The Internet of Things (IOT) is presently a fast catching paradigm in which the everyday objects are manufactured with essential capabilities such sensing, networking and processing. These capabilities enable them to communicate with one another and with other devices and services over the Internet to complete some objective. One of the most important issues is security. When devices are given the freedom to talk to each other, then there are immense possibilities of misuse. In this paper, we propose a secure communication approach for device-to-device communication. It is an Identity-based encryption approach which includes revocation of keys if misuse is detected. The proposed method takes into consideration the high probability of misuse and hence malicious devices are identified and eliminated. This paper presents the design of the proposed approach along with a first level implementation using Java and MsAccess.

***Keywords*:** Internet of Things, communication, Internet

1. INTRODUCTION

The Internet of Things (IOT) has become an important topic in engineering circles and technology-based industries. This technology is an inherent part of a numerous networked

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

products, sensors and systems which are being manufactured with the current electronics miniaturization approaches. Basically IOT is the facility and technology used to connect a wide range of computing/communication devices or gadgets. These devices can be remotely managed and controlled, thus moving towards a magical world of do-anything-from-anywhere.

This may sound like science fiction, but the reality is, today it is possible to use IOT technology to "see" buildings for sale from your mobile or your laptop. Thus a buyer can "see" houses from various angles before deciding which one to buy. IOT technology is offering the possibility to transform all sectors such as industry, agriculture, healthcare, entertainment, etc., by increasing the availability of information along a different dimension using networked sensors [Carolyn Marsan et. al.].

The advantages of the IOT technology are that it offers communication, control and automation, monitor, and information. Also it saves time and money, offering an efficient and better quality of life. The main problems of IOT are compatibility, complexity, privacy and security. From the security perspective, the following issues are evident.

Networking Challenges: Today's networking technology was not designed to support large numbers of computing/communicating gadgets. Further complication is because these devices are low-power devices that interact with the human users, physical world, and the cloud in complicated ways. These requirements cause major research challenges in the area of networked systems, specifically in terms of scalability, open network interfaces and multitenancy [Rajeev Alur et. al.].

Security Challenges: Additional challenges are due to the devices being diverse, interacting, and potentially unsecure, security threats from ubiquitous devices, system-wide security abstractions.

In this paper, we present one approach to secure the IOT environment, specifically the communication between IOT devices. In Section II, some of the security requirements for IOT environment and the prevailing research work are discussed. In Section III we describe the proposed identity based encryption with secured outsourced revocation for IOT environment. The results are given in Section IV and concluded thereof.

2. SECURITY OF INTERNET OF THINGS

IOT devices are typically wireless and may be setup in public places and are made secure using end to end encryption. Encryption is also used for information security in the IOT environment. Every IOT device must be secured throughout its lifecycle by providing secure booting, access control, authentication of the device, firewall, and regular patches. A typical IOT communication environment is depicted in Figure 1.

Security in this environment must be in terms of authentication and secure communication between (i) mobile-app and cloud services, (ii) cloud services and the backend web applications and (iii) device to device communication.

In this paper, we propose the identity-based encryption mechanism with revocation for secure device-to-device communication.

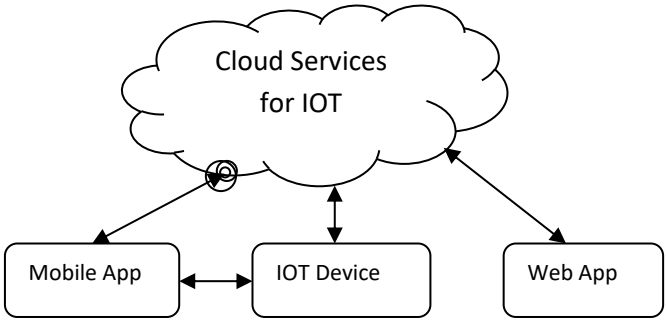

Fig. 1. IOT Communication Environment

3. DENTITY BASED ENCRYPTION WITH SECURED OUTSOURCED REVOCATION FOR IOT ENVIRONMENT

Identity-Based Encryption (IBE) is an alternative of public key encryption. The major advantage is simplified key management in a certficate based Public Key Infrastructure (PKI) by using human-unique identities for e.g., name, email address, IP address, etc. as public keys in Private Key Generator. In the IOT environment the devices are the users. After generation of keys the Private Key Generator communicates to the user (IOT device or the mobile device). Because of this, the physical devices are able to stay linked. If both device are authenticate PKG serves the device2 keys. The message (M) can be transfer to device1 to device2 is shown in Fig. 2

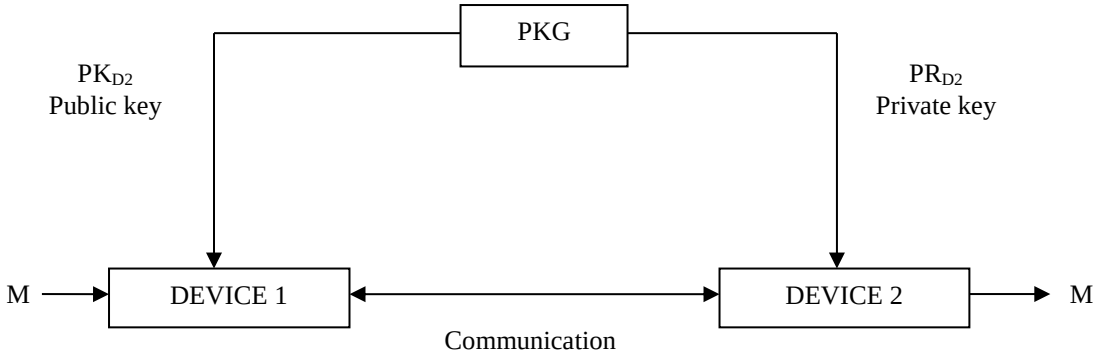

Fig. 2. IOT device-to-device

During a misdeed, i.e., when any device if found to misbehave, then the central key management system (the PKG) will revoke the keys of the misbehaving IOT device. This is known as revocation and is shown in Fig. 3. Normally, all the users despite the consequences of whether their keys have been revoked or not, have to make contact with PKG frequently to prove their identities and update new private keys. It requires that private key generator is online and the protected channel must be maintained for all communication.

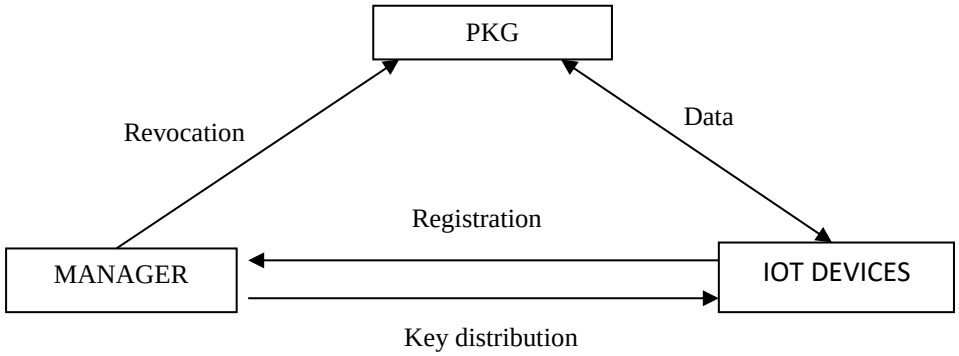

Fig. 3. Revocation process in IOT

Key Update Cloud Service Provider (KU-CSP) is a central system used for outsourced revocation. This is shown in Figure 4. The KUCSP updates the users key each and every time when ever the user needs. KU-CSP mostly operate key generation related operations during key-update and key-issuing processes. KU-CSP leaving only an invariable number of uncomplicated operations for PKG and users to do locally.

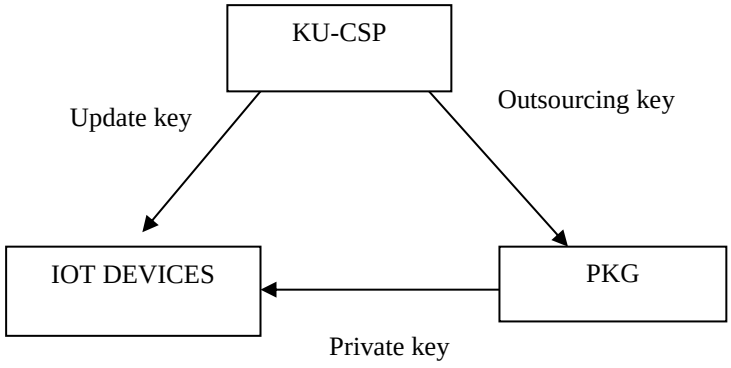

Fig. 4. System model of IBE with outsourced revocation for IOT environment

PROPOSED MODULES

The IOT communication is considered as a three stage communication – (i) registration of a device (ii) communication between the registered devices under secure conditions and (iii) communication between the registered devices under revoked conditions.

(i) REGISTRATION MODULE

In this module, the new IOT device registers with the PKG. The PKG would generate and provide the (public key, secret key) pair to the new users, entering into the system. Key generation is done with random prime numbers to generate a unique (public key, secret key) pair.

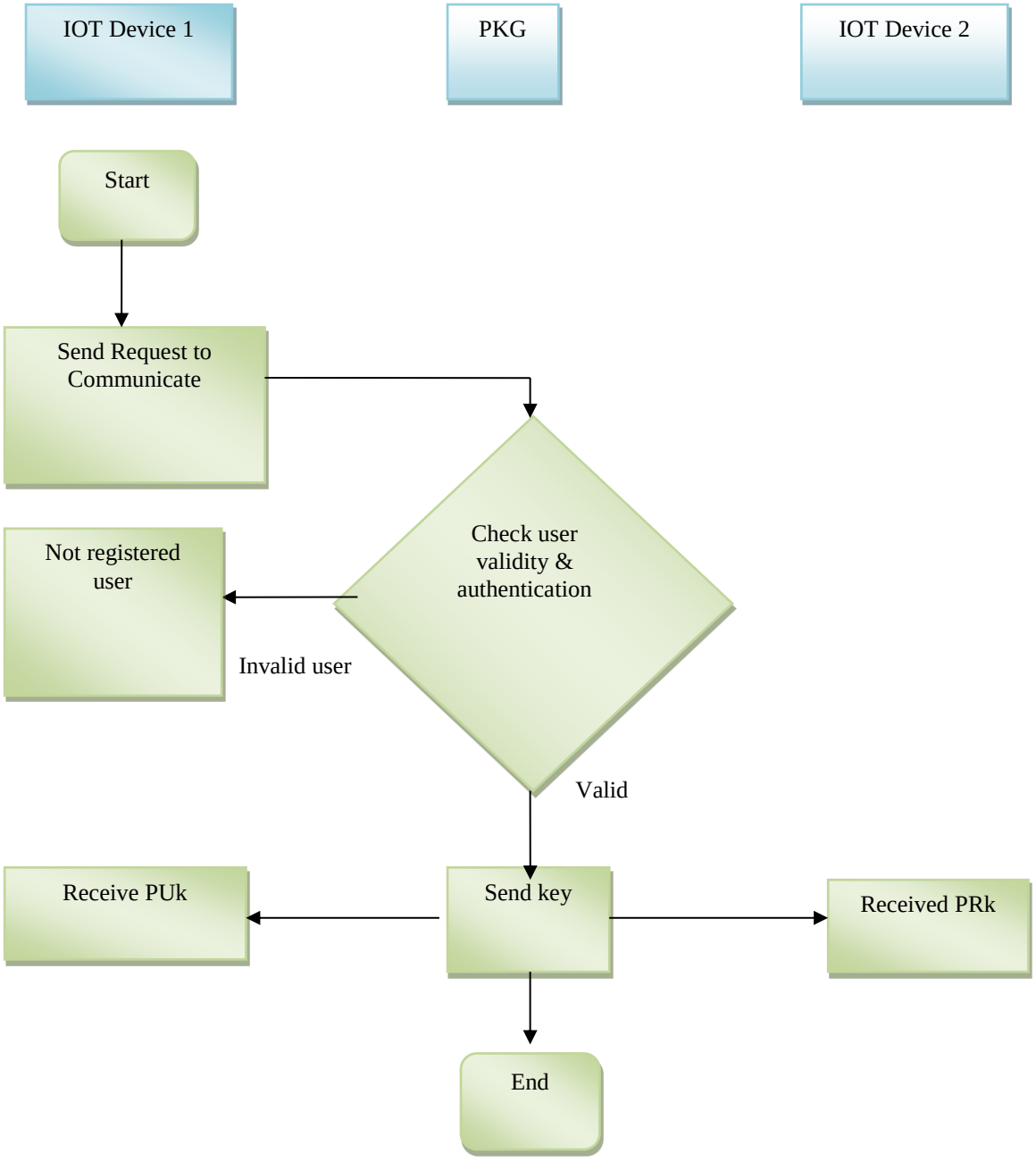

Fig. 5. Registration Module

(ii) SECURE COMMUNICATION

In this module to check whether the users are already registered. If there is registered user means PKG send their public key to both client and server. Using the key they perform send and receive function. If there is not registered user means PKG says invalid user.

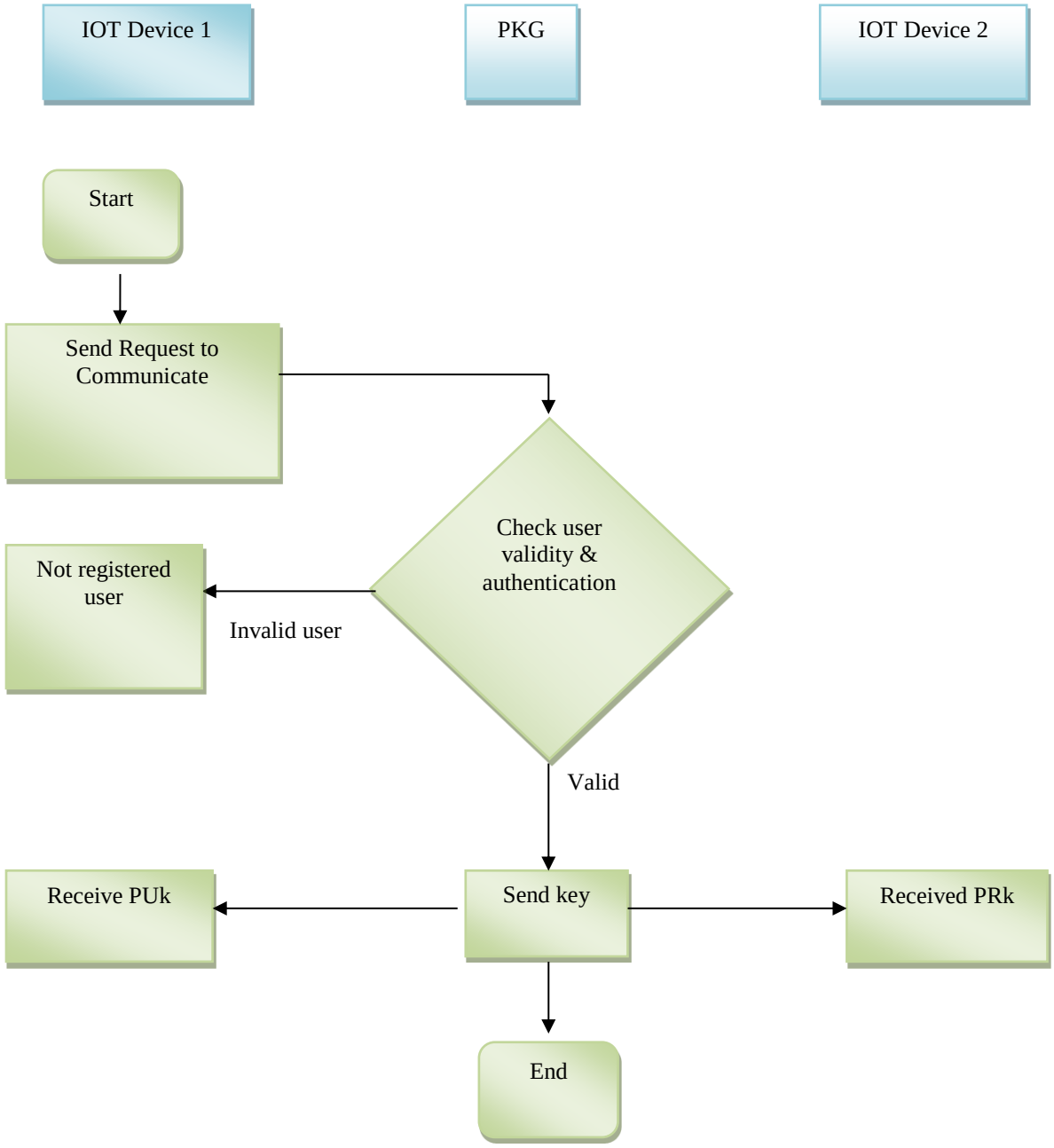

Fig. 6. Secure communication between two IOT devices

(iii) REVOKED CONDITION

The misdeed algorithm run by PKG. It takes as input from the user, a valid user list and the set of identities to be misdeed. Before that PKG check the user data in database. The misdeed process run PKG, after the process PKG send message to user and update their database.

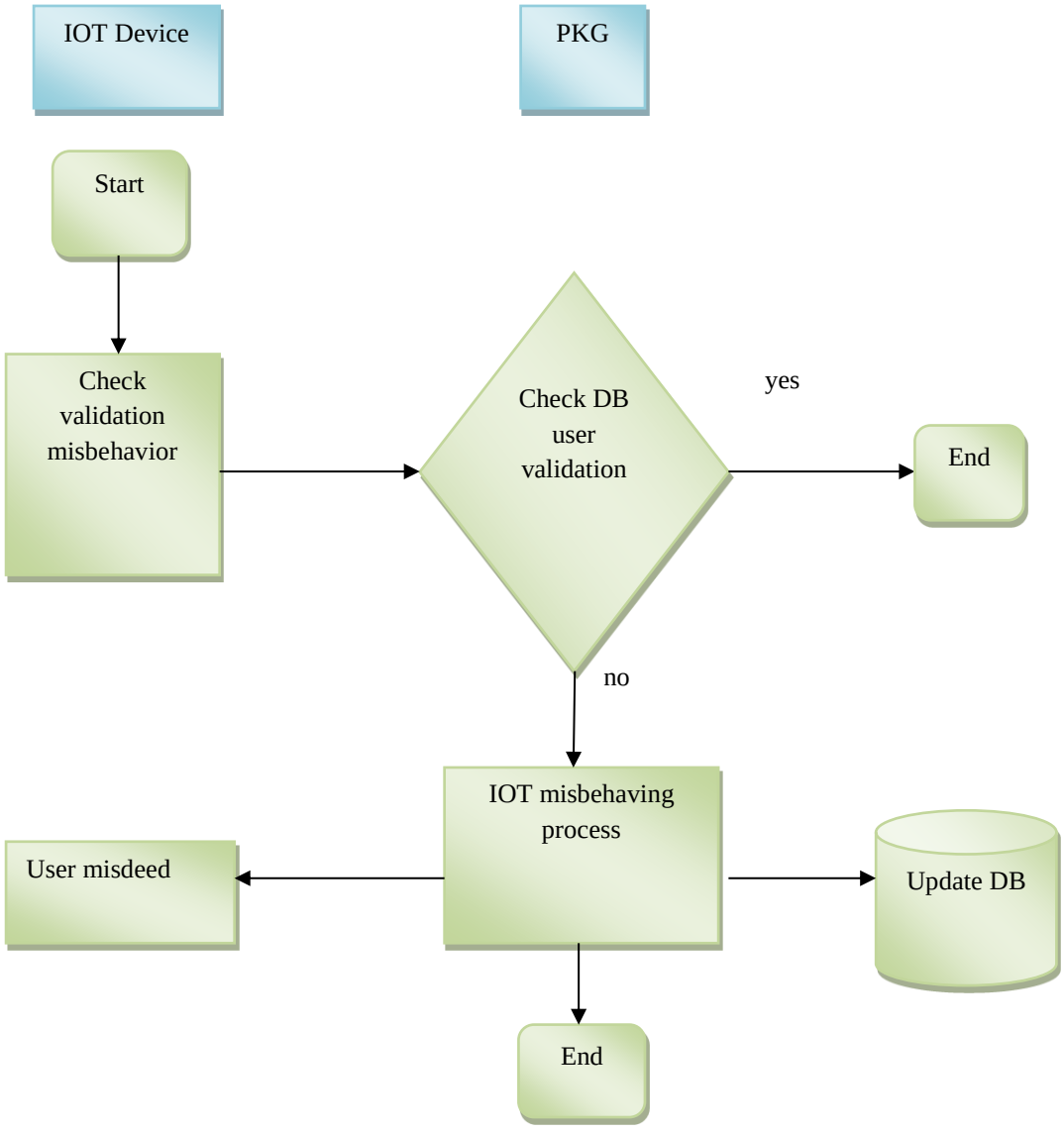

Fig. 7. Misdeed process

PSEUDOCODE

```
Procedure process_msg(in)
{
        Msg=substring(in.readUTF());
        If msg==”REG_REQ” then
                If found(user in db) then
                        invalid user registration
                Else
                        Generate key()
                        Update DB with new user
                        Send PUk to user
                endif
        Elseif msg==”REQ_SND”
                If found(user in DB)
                        Then get key from DB
                        Send PUk  to user1 ,PRk to user2
                Else
                       unauthenticated user
                       //can not be communicate
                Endif
        Elseif msg==”REQ_RCV”
                If found(user in DB)
                        Then get key from server
                        Receive data
                Else
                        Not REQ_RCV message
                Endif
        Elseif msg==”MISDEED”
                If found(Check user validity)
                        //if user in DB
                                IOT misbehaving process
                        Update DB (user misdeed)
                        //else not REG-REQ
                        Send message to client (user misdeed)
                Else
                        Not registered user
                Endif
        Endif
}
```

Fig. 8. Pseudo code for IBE with outsourced revocation for IOT environment

If the below screenshots show the little work of IBE project by using java and ms-access.in future we develop the IBE project is in secured communication. The java programming language is a high-level language. The java programming language is unusual in that a program is both compiled and interpreted. The java is a platform it has two components they are the *java virtual machine*, the *java application programming interface*. Ms access is a database management tool that enable one to have good command of data collected in windows system. The programmer enables one to sort, retrieve, summarize and report results speedily and efficiently. It can combine together data from various files through creating relationships, and can make data entry in well-organized and accurate.

SCREENSHOTS

i. REGISTRATION

New IOT device registers with the Private key generator. The PKG would create and provide the key pair to the new users while entering into the system. Key generation is done with random prime numbers to generate a unique key pair in PKG.

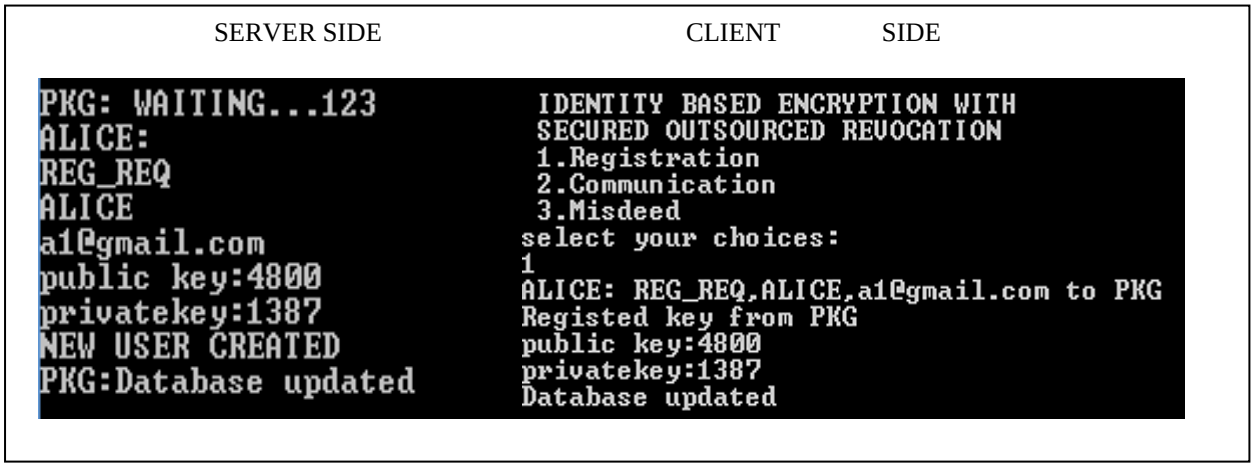

Fig. 9. Registration of user

ii. COMMUNICATION

Difficult to construct the key pair(public key and private key) to ID based key sharing scheme.ID based cryptosystem can modifies the keys ID based public key to the authentication purpose. ID based cryptosystem with authenticate it cannot stop the receiver from substituting a new message from the encrypted message.

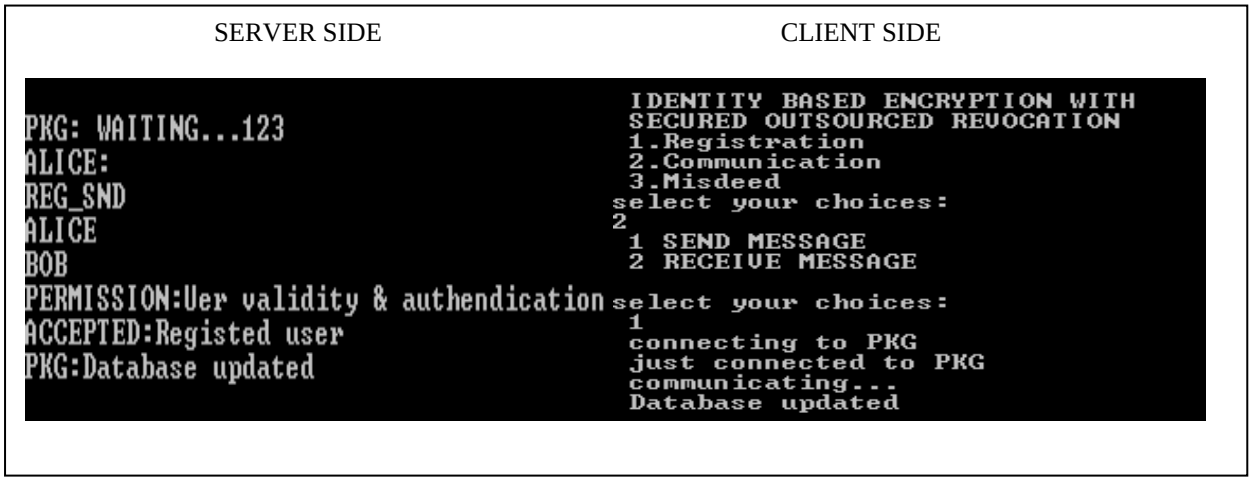

Fig. 10. Communication request to pkg

iii. MISDEED

IBE, there has been little work on studying the misbehaving IOT device mechanisms. Propose a way for the users to sometimes renew their private keys without interacting of PKG. The PKG publicly post the key update information, which is much more convenient to users.

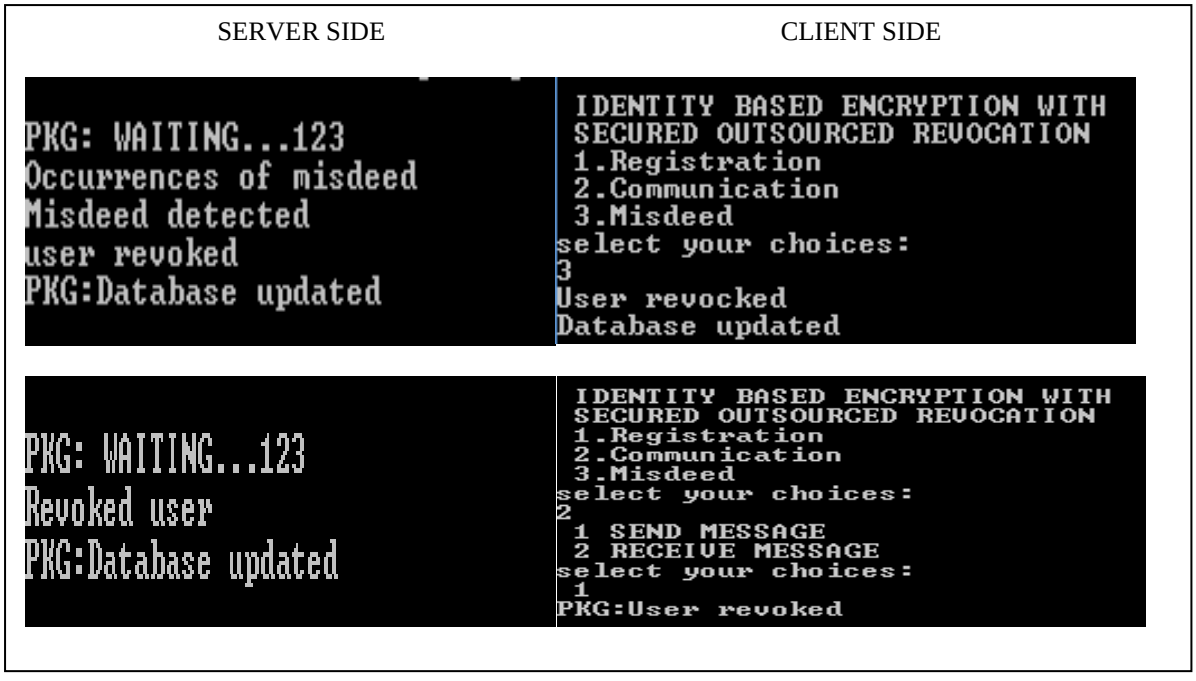

Fig. 11. Communication request after the user misbehaving IOT device

4. CONCLUSIONS

The internet has significantly changed the way we live, and today much interaction is among the internet of things. Our mobile phones, household appliances, vehicles, etc. can communicate with each other. Among the various issue concerned with the IOT, security plays a vital role. The freedom available with the devices in the IOT, to talk to each other, is a major threat to security. When misused, this freedom can lead to miscreants creating havoc. In this paper, we proposed a secure communication approach for device-to-device communication. It is an Identity-based encryption approach for confidential communication between sender and receiver. The method also includes revocation of keys if misuse is detected. The fact that there is a high probability of misuse of *freedom to communicate* in IOT we have included revocation and thus malicious devices can be identified and eliminated. The design of the proposed approach along with a first level implementation using Java and MsAccess had been presented in this paper. As future work we propose to implement the complete algorithm on a network simulator and test with multiple devices.

References

[1] Harald Sundmaeker, Peter Friess, Patrick Guillemin, Sylvie Woelfflé, Vision and Challenges for Realising the Internet of Things, Cluster of European Research Projects on the Internet of Things, March 2010. Publications Office of the European Union, 2010 ISBN 978-92-79-15088-3, doi:10.2759/26127

[2] Rajeev Alur, Emery Berger, Limor Fix, Kevin Fu, Gregory D. Hager, Klara Nahrstedt, Elizabeth Mynatt, Shwetak Patel, Daniel Lopresti, Jennifer Rexford, John A. Stankovic, Ann W. Drobnis, and Benjamin Zorn, Systems Computing Challenges in the Internet of Things, computing community consortium, September 22, 2015. arXiv:1604.02980

[3] Carolyn Marsan, Michelle Speckler, The internet of things: An overview. Internet Society, October 2015.

[4] J. Li, J. Li, X. Chen, C. Jia and W. Lou, Identity-Based Encryption with Outsourced Revocation in Cloud Computing, in *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425-437, Feb. 2015, doi: 10.1109/TC.2013.208

[5] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, Identity-based Encryption with Efficient Revocation, *14th ACM Conference on Com- puter and Communications Security*, CCS 2008, ACM Press, 2008.

[6] Ryuichi Sakai, Maseo Kasahara, ID based cryptosystems with paring on elliptic curve, Osaka Electro Communication University, Japan.

[7] Herbert Schildt, java complete references, Tata Mc Graw Hill Ltd, New Delhi, 2008.

[8] Mr. Gordon Moore, Dr. Jahangir Alam, Velma Latson, www.tutorialspoint.com

[9] www.java-examples.com

[10] www.beginnerbook.com