IIOAB JOURNAL
ISSN: 0976-3104

ARTICLE

IOT APPLIANCE ACCESS STRUCTURE USING ABE BASED OTP TECHNIQUE

Suraj U. Rasal[1*], Raghav Agarwal[1], Varsha S Rasal[2], Shraddha T. Shelar[3]

[1]*Computer Engineering Department, Bharati Vidyapeeth University College of Engineering Pune, INDIA*

[2]*Dept. of Computer Science & Engineering, Nehru College of Engineering & Research Center, Thrissur Kerala, INDIA*

[3]*Dept. of Information Technology, D.Y. Patil College of Engineering Akurdi, Pune, INDIA*

ABSTRACT

Internet of Things refers to the use of standard Internet protocols for the communication of embedded system. Even though certain security techniques are applied like cipher text, Attribute Based Encryption, IoT is less secured which shows need to improve security level. Overcoming with drawbacks in existing security approaches, multiple security approaches are applied to improve security in IoT. Randomized selection logics are applied to select attributes randomly. One time password is generated based on same selected attribute data set. Based on selected data, RSA algorithm is applied to form primary and secondary encrypted keys. IoT appliance access structure is applied with those multiple security approaches to enhance security level.

KEY WORDS
IoT(Internet Of Things), ABE(Attribute Base Encryption), CABE(Current Attribute Based Encryption), R_D(Randomized selection algorithm), OTP (One Time Password)

Received: 7 Sept 2016
Accepted: 28 Sept 2016
Published: 29 Sept 2016

***Corresponding Author**
Email:
surasal@bvucoep.edu.in
Tel.: +918793000079

INTRODUCTION

The time is continuously changing so do the internet .With the help of Internet of things now machine can communicate with each other, IOT provides connectivity for everything and everyone, IOT is so much advance that they can actions on their own. But there are many security flaws in IOT so we will use ABE(Attribute based Encryption) to cover as many security flaws . Attribute based Encryption we use it or the log encryption schemes that represent user attributes as a monolithic set in keys instead of encrypting each log file with diff key. To access a particular file we need that specific attribute to decrypt that file .So we can use ABE encryption mostly on the databases , as databases are one of the most important as it contains very sensitive and personal data so to secure this we will use ABE encryption. A first step in addressing this problem of trust is to only store information in encrypted form. However, data access is not static – as employees are hired, fired or promoted so every time we cannot change the credentials of the database but it will be necessary to change the authority who can access the data . SAP HANA is one most used databases now a days by automobile company and they have every personal info about their customer, so if anybody may be able to penetrate the server and bypass authentication by exploiting software vulnerabilities [1]. So the solution to this is Cryptography we can access the control through Attribute based Encryption (ABE). For Instance in the Ubiquitous IoT application such as smart city, data is usually gathered by many people of different domain [2]. The data may be out without the knowledge of the user and transmitting in the plain text , there may be many departments and the data may be transferred inter department that can be accessed by an unauthorized user and can cause serious problem. Our main area of Interest here is to exploit the heterogeneous nature of the IoT to make best possible use of Attribute based Encryption Schema in diff environment.

MATERIALS AND METHODS

Internet of Things: Security Architecture

IoT have some security flaws so here we are going to see the architecture of the Internet of Things. Every Network has same security issues whether its mobile communication network, Internet, Sensor networks etc. The main challenge in IoT security is Data and privacy protection. In IoT our main communication is done through RFID (Radio frequency identification) and WSN (Wireless Sensor Network) so all the data travelling through these communication channels are encrypted in some or the other format [3]. The other end users have to confirm their identity so see the data. There are some issues for the security of the IoT, one of the issues is the related technologies to IoT for constructing and implementation of network function and the other issue is the IoT itself, the main issues with IoT is the compatibility issues between different networks this is prone to security. In the network due to large amount of data transfer any one can create data congestion which can cause of data loss. So we should look into the problem regarding connectivity problem and network redundancy. Internet of Things connects with people daily life, to ensure technology security and to strengthen human awareness [4]. IoT is usually divided into three layers, Application Layer, Transport layer & Perception Layer. Application Layer is subdivided into two sub parts IoT Application &Application support Layer. Transportation layer is subdivided into three sub parts viz. Local area network, Core network & Access network. And Perception Layer is subdivided into two sub parts Perception Network & Perception Nodes. Each technology has some specific role which is not

IIOAB JOURNAL
ISSN: 0976-3104

irreplaceable by anyone else. Each layer has different security measure every layer secure different networking protocols as perception layer secures RFID security, WSN security, RSN security and many more. Transport Layer secures Internet security, Local Area network security, wi-fi security, GPRS security. Application layer includes application support layer and specific IoT applications. The security in support layer includes middleware technology security, cloud computing platform security. IoT in different industries have different application and different security measure [5].

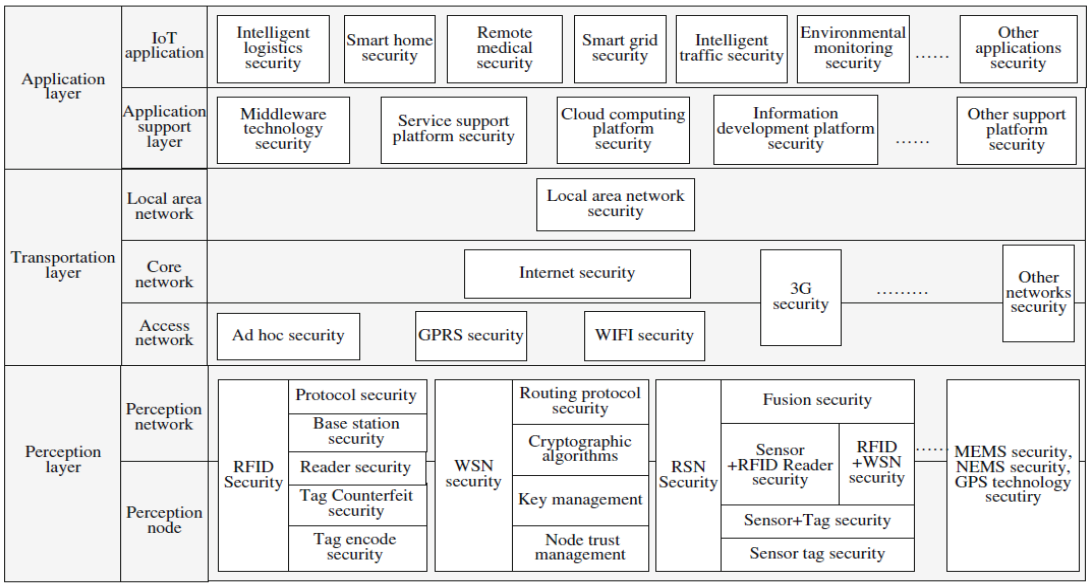

Fig.1: Security Architecture in IoT [4]

Cryptographic Approaches

There are many Cryptographic algorithm are widely available now and some of them are used right now by many company and some of them have been applied to secure the internet protocols. As shown in table we have four type of algorithm available for encryption. For confidentiality data encryption we basically use Advance Encryption Standard (AES), it is basically symmetric encryption data. There's another algorithm its purpose is to generate digital signature and key transport, it is one of the frequently used algorithm know as RSA/ECC [6].

Table 1: Cryptographic Algorithms [6]

ALGORITHM	PURPOSE
AES (Advanced Encryption Standard)	Confidentiality
RSA (Rivest Shamir Adelman) / ECC (Elliptic Curve Cryptography)	Digital signature key transport
DH (Diffie-Hellman)	Key Agreement
SHA (Secure Hash Algorithm)-1/ 256	Integrality

An algorithm is made to generate for the key arrangement know as the Diffie Hellman (DH). The problem for integrity has been solved by the SHA-1 and SHA-256 secure hash algorithms [6]. These algorithms can be applied only if all the required resources are available memory and processor, but the part of implementation is still under research.

Attribute Based Encryption

As most data on the internet is shared by the third party websites, so we need to encrypt the data secure which is kept at the websites. Normally a person is identified by a unique identifying string, but Attribute based Encryption scheme in contrast is a scheme in which a string is identified on the basis of the attributes and some function are used to decrypt this cipher text [7]. In Attribute based Encryption it allows user to set policy describing who should be able to the data. In this solution set of attributes and cipher text is associated with formula over attributes; the other end user will be able to decrypt the cipher text if and only their private key matches attribute which satisfy the formula. It is one of a special case of function encryption as this can be practiced in real life [8].

IIOAB JOURNAL
ISSN: 0976-3104

Cipher text Policy

It is a type of identity based encryption. In cipher text policy attribute based encryption (CP-ABE), every secret key is associated with a set of attributes and every cipher text is associated with an access stricter of attributes [9]. It has one public key and has a master key and it use to make more private keys. However, CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher texts [10]. It is much more secure but it does not have flexibility and new key must be generated for each file this is because many file with same key won't give fine grained access [11].

WORKING APPROACHES IN INTERNET OF THINGS

Centralized Internet of Things

In centralized Internet of things all the devices (i.e. network of things such as mobile phones, radiation sensor, cars, home automation system) which have some computing power and which can be connected to internet to a dedicated central server know as centralized internet of things. Their only task is to provide the data and all this data is retrieved by the single central entity. Now all these data is processed in to information. User won't be able to make use of IoT services until he connects to the Internet provided by the central entity. Centralized entity can be formed by using a server or by cluster of devices forming a cloud [12].

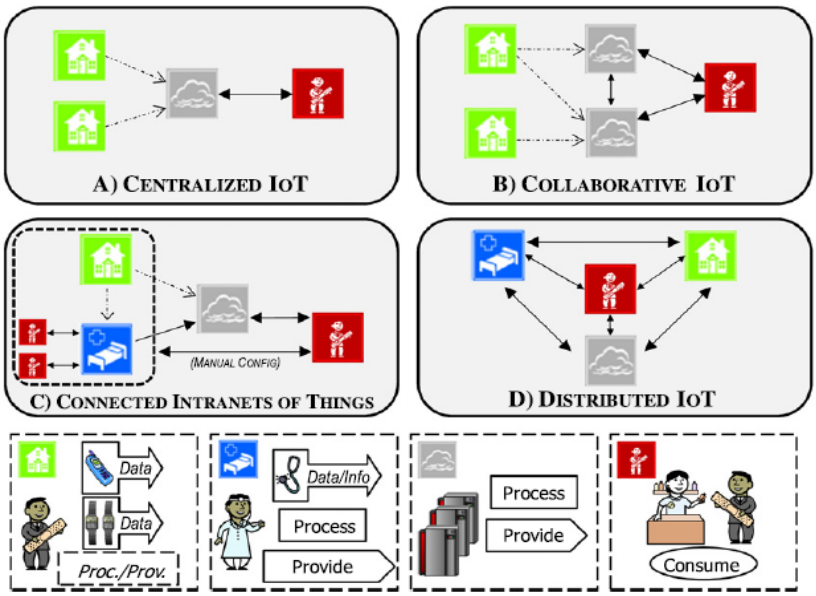

Fig.2: Approaches in Internet of Things [12]

Collaborative Internet of Things

Collaborative Internet of Things is not very different from Centralized Internet of Things as power to take decision is still with central entity. In Collaborative Internet of things there are many central entities instead of one. These all the central entity interacts with each other and they share the data between, different central entities are made up for specific task is performed by each. As a result, various central entities that can exchange data and information with each other for generating new services. For example IoT service provider that analyzes the radiation in atmosphere can now collaborate with diff cities to find the radiation in atmosphere of the whole country [12].

Connected Intranets of Things

In data acquisition (INTRANET OF THINGS) it process local information and shares the data with both central entities and to the local user. There is no relation between the collaboration of entities. The whole data flow from the central entities from where get the complete view of the whole system. This is a big security flaw or we can say a loophole because any local user can access the personal data of anyone [12].

IIOAB JOURNAL
ISSN: 0976-3104

Distributed IoT

The name itself indicates that all the entities can access, retrieve, process, and combine all the information to other entities. As time is evolving so does the Intranet of Things as it is evolved from remote entities to fully functional entities. It can now be collaborated with local entities for the betterment of the society and centralize cloud service. So this is beneficial for the society they can check any service is available right from their home [12].

SECURITY ISSUES IN INTERNET OF THINGS

Security is one of the major aspects of Internet of Things. Because whenever we say internet the first thing that comes in mind is security because as soon as anything gets connected to internet we can say we are connection to the rest of the world through a network and on this planet there is no device which is totally secure so there are some security measure we have to take to secure Internet of Things. If anybody can get unauthorized access to Internet OF Things it can be dangerous as Internet of things have full permission to do anything. So there are some basic measure authentication, authorization, and access control [7].

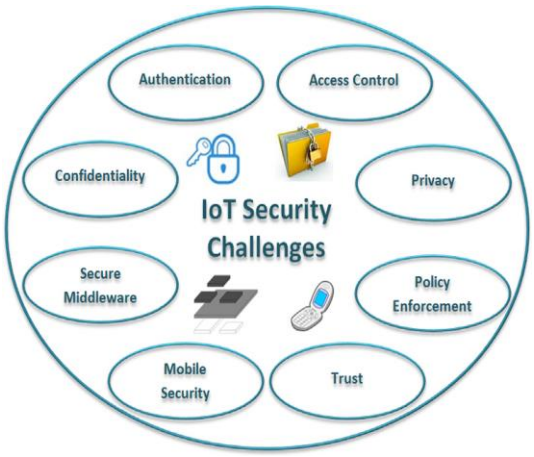

Fig.3: Security Challenges in IoT [7]

In authentication a user is given with a specific user id and the password until and unless he enters that specific credential he won't be allowed to access the data. These credentials are confidential so they should be kept personal and should not be shared with someone else. Authentication makes the use of custom encapsulation mechanism namely intelligent service security Application protocol. It has cross-platform communication with encryption signature and authentication to improve the security. It is based on two-way authentication security scheme and it is placed between transport layer and application layer. Currently authentication is based on RSA Algorithm; these all things provide confidentiality and authenticity. We can check our confidentiality and integrity by analyzing how Key Management System could be applied to the to the IoT context. There is another approach Object Naming Service (ONS), which helps us to identify security requirement (trustworthy and attack resistance) whether our devices is capable of these types of attacks or not. The key is establish on the basis of Elliptic curve cryptography (ECC), this is another method for the light weight encryption mechanism, this is one of the schemes that define Attribute based access policies managed by attribute authority[7] . By this we can use Authentication and confidentiality.

Access control refers to the access given to a particular user to access the data, the access is given depends upon the authority of the user. This access list is defied at the database which checks every credential of the user and allows the type of access to him. The client subsystem helps in user authorization so no other user can access unauthorized data [7].

RESULTS

One time password is latest cryptographic trend in the sensitive online transactions. Attribute Based Encryption is widely used technique. In proposed approach, both cryptographic techniques are applied simultaneously. Internet of things uses security approach at some extent. Multiple IT appliances are included in internet of things which requires multiple security approaches to enhance its security level.

IIOAB JOURNAL
ISSN: 0976-3104

User credentials

IoT application layer is used as a part of user interface through which user credentials are accepted. Based on accepted user credentials, next procedure is started. User credentials are considered to authorize and identify user [13]. IoT application layer is installed in respective IoT devices which will create common interface to securely access devices. Logical system understands according to authorized user and respective devices.

Attribute selection

Based on IoT device and user credentials identification, attributes are used. Attributes are allocated according to these two entities considered as device used and user credential. While designing setup and synchronizing it with server, attribute allocation is done. For example if printer P is considered and User U is accessing based on IoT, respected attributes will be considered. Attribute set includes all attributes related to considered user and IoT appliance. Particular user has regarding attributes and IoT based appliance has regarding attributes.

Attribute Allocation

Based on user, attribute sets are created. U_1, U_2, U_3, U_4,.....,U_n are registered user sets which has respective attributes based on user credentials and registered user details [13]. Also devices or appliances which have secure access based on IoT, are registers according to attributes sets and respective attributes. D_1, D_2, D_3, D_4, D_5,....,D_n are attribute sets according to IoT appliances.

$U_1 = \{ U_{11}, U_{12}, U_{13}, U_{14},...., U_{1n}\}$
$U_2 = \{ U_{21}, U_{22}, U_{23}, U_{24},...., U_{2n}\}$
$U_3 = \{ U_{31}, U_{32}, U_{33}, U_{34},...., U_{3n}\}$
.
.
.
$U_n = \{ U_{n1}, U_{n2}, U_{n3}, U_{n4},...., U_{nn}\}$

User attributes are allocated accordingly. User attribute sets are created according to user registration.

$D_1=\{ D_{11}, D_{12}, D_{13}, D_{14}, ..., D_{1n}\}$
$D_2=\{ D_{21}, D_{22}, D_{23}, D_{24}, ..., D_{2n}\}$
$D_3=\{ D_{31}, D_{32}, D_{33}, D_{34}, ..., D_{3n}\}$
.
.
.
$D_n=\{ D_{n1}, D_{n2}, D_{n3}, D_{n4}, ..., D_{nn}\}$

Here, attribute sets and attributes are allocated according to registry done in the attribute storage database. Here U_1 may be any user who has some user credentials, and user details. Based on user details, attributes are allocated [14].

U_1={'name','mob','city','dob',.....}
Where 'name'=U_{11}.
D_2={'D_name','D_MAC','D_reg.date','Company',.....}
Where, 'D_name' = D_{11}.

In similar ways rest of the user components are allocated and stored accordingly [14]. If user has entered user details, accordingly user attributes are selected from attribute set. If U_1 is user and respective user attributes are as per attribute sets, these will be selected randomly by using randomized selection algorithm R_D. In this case, attributes selected can be U_{11}, U_{13}, U_{15}, U_{16}. There is no any specific logic is applied for attribute selection. Even there is possibility of same attribute selection in next attempt. Even though, in case of device attribute selection same thing is applied. Logic depends on the randomized selection algorithm. Device or appliance attributes can be selected according to applied logic such as for device D_2 , randomly attributes can be selected as D_{21}, D_{23}, D_{24}, ..., D_{2n}.

$U_n \xrightarrow{R_D} U_{nf}$

$D_n \xrightarrow{R_D} D_{nf}$

IIOAB JOURNAL
ISSN: 0976-3104

Based on randomized selection algorithm, finalized sets U_{nf} and D_{nf} are formed which are considered as final attribute sets to apply encryption techniques. Rest of the device attributes are allocated and stored accordingly.

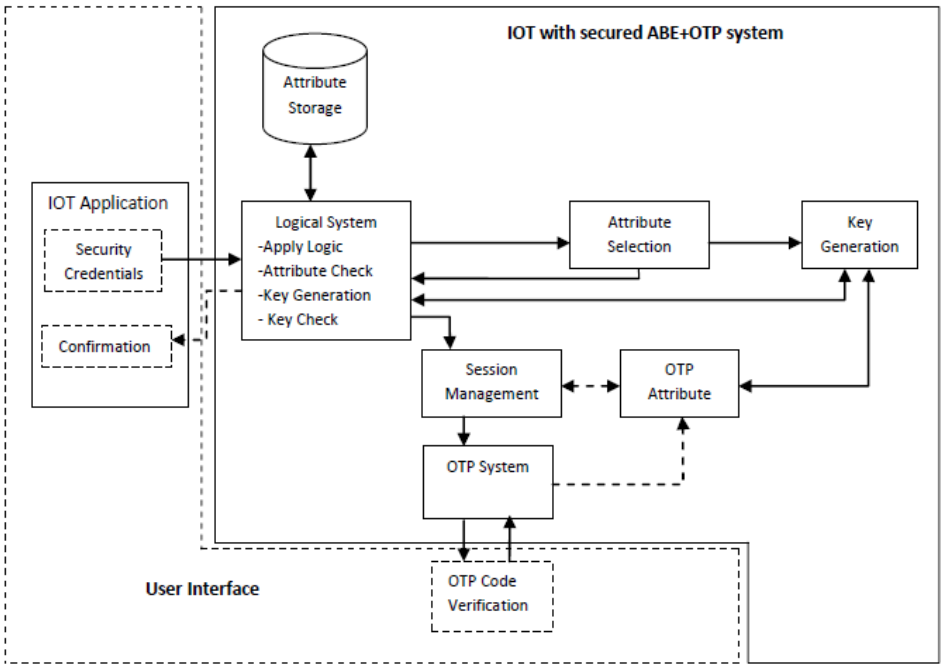

Fig. 4: IoT with Secured ABE+OTP System

Main attribute set formation

After attributes selection, finalized attribute sets are added to form main attribute set. Main attribute set is formed to from finalized attribute sets. In this paper, two algorithms are applied. While selecting attributes, randomized sort algorithms is applied. And RSA algorithm is applied to form encrypted data [15]. To provide an access to the IoT based appliance, these encrypted formatted data is verified. At the application layer side, encryption as well as decryption is done. Consider user attributes and devices attributes are selected as U_{11}, U_{13}, U_{15}, U_{16} and D_{21}, D_{23}, D_{24}, ..., D_{2n} respectively. Attribute sets are combined further to form main attribute set A_n.

$A_n = U_{nf} + D_{nf}$
$A_n = \{ U_{11}, U_{13}, U_{15}, U_{16}, D_{21}, D_{23}, D_{24}, ..., D_{2n}\}$

RSA algorithm is applied to process formed attribute set [1]. After applying RSA algorithm, main data is encrypted based on which encrypted key is generated [15].

$A_n \xrightarrow{RSA\_E} E_{An}$

Here E_{An} is an encrypted key. This encrypted key is called as primary key. Important condition to access IoT appliance is, primary key should be equal to the secondary key. Secondary key is generated according to the One Time Password elements set.

OTP approach

Based on selected attribute, One time password is generated. One time password is a combination of numbers, alphabets and special characters. Attribute allocation table is formed while installing IoT application layer. Each attribute is allocated with some special character. According to selected attributes, numbers, alphabets and special characters are allocated and OTP set O_s is formed. For above example, it can be,

$A_n = O_{S\backslash} = \{ U_{11}, U_{13}, U_{15}, U_{16}, D_{21}, D_{23}, D_{24}, ..., D_{2n}\}$
$O_S = \{ '1','9','7','3','X','A','@',.....,'\$'\}$

User has to enter OTP elements to validate him as an authorized user. Based on one time password, encryption key is generated. This encrypted key is called as secondary key.

$O_S \xrightarrow{RSA\_E} E_{Os}$

IIOAB JOURNAL
ISSN: 0976-3104

Since same encryption algorithm is applied on same attribute set with same attributes sequence, generated key is similar to the primary generated key.

$E_{An} = E_{Os}$

To identify the equality between two keys, decryption modules are applied on both sides. IoT application layer has encryption as well as decryption module. In decryption module, encrypted data is decrypted and it will automatically provide access to the requested IoT appliance.

E_{An} RSA_D A_n

E_{Os} RSA_D O_s

But $A_n = O_s$

After attribute based details checking, it is confirmed that both primary and secondary keys are same. Then only IoT based user has access to the requested IoT appliance.

CONCLUSION

In proposed approach user and appliance attributes are used instead of actual data which shows data hidden approach. Selected attributes are used using randomized selection algorithm, shows situation based attribute selection method. One time password is generated based on selected attributes in terms of different ASCII sets. It increases levels in user authorization and validation process. Encryption key is generated using RSA algorithm where proposed approach based data is used. Combining these approaches simultaneously including attribute allocation, selection, applying encryption algorithms and One time password, enhances the security level to access IoT appliances.

CONFLICT OF INTEREST
The authors declare no conflict of interest

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None

REFERENCES

[1] Rasal, Suraj U, et al.[2016] Improving Security in SAP-HANA Cloud by Applying Multiple Encryption Policies ,*International Journal of Science Technology & Engineering* . 196-200.

[2] Zhang, Zhi-Kai, et al. [2014] IoT security: ongoing challenges and research opportunities. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. IEEE.

[3] Kahate, Atul. [2013] *Cryptography and network security*. Tata McGraw-Hill Education.

[4] Jing, Qi, et al. [2014] Security of the internet of things: Perspectives and challenges, *Wireless Networks* 20.8 Springer : 2481-2501.

[5] Stallings, William. [2006] *Cryptography and network security: principles and practices*. Pearson Education India.

[6] Suo, Hui, et al. [2012] Security in the internet of things: a review, *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*. IEEE Vol. 3.

[7] Sicari Sabrina et al. [2015] Security, privacy and trust in Internet of Things: The road ahead." *Computer Networks* 76 Elsevier 146-164.

[8] Yao Xuanxia, Zhi Chen, and Ye Tian. [2015] A lightweight attribute-based encryption scheme for the Internet of Things." *Future Generation Computer Systems* 49 Elsevier: 104-112.

[9] Han Jinguang, et al. [2015] Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. *IEEE Transactions on Information Forensics and Security* 10(3): 665-678.

[10] Rao Y. Sreenivasa, and Ratna Dutta. [2013] Decentralized Ciphertext-Policy Attribute-Based Encryption Scheme with Fast Decryption, *IFIP International Conference on Communications and Multimedia Security*. Springer Berlin Heidelberg.

[11] Touati, Lyes, Yacine Challal, and Abdelmadjid Bouabdallah. [2014] C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internet of things, *Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on*. IEEE.

[12] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. [2013] On the features and challenges of security and privacy in distributed internet of things, *Computer Networks* 57.10 Elsevier: 2266-2279.

[13] Rasal, Suraj, Sanya Relan, and Karan Saxena. [2016] OTP Processing using UABE & DABE with Session Management, *International Journal of Advanced Research in Computer Science and Software Engineering* : 57-59

[14] Rasal, Suraj, Megha Matta, and Karan Saxena. [2016] OTP system with third party trusted authority as a mediator, *International Journal Of Engineering And Computer Science* 16566-16568

[15] Burnett Steve and Stephen Paine. [2001] *The RSA Security's Official Guide to Cryptography*. McGraw-Hill, Inc.