A New Scheme to Safeguard Data for Cloud Integrated Internet Things

Bingu Rajesh, Puvvada Nagesh, Koppada Gowtham, Gorantla Vivek, N.Srinivasu

Abstract*: *In our day-to-day life people use many electronic gadgets to control things around, which in turn those things communicate with other things around and get the requested work done, this is Internet of Things. As there would be enormous amount of data generated by Internet of Things why not we store it in cloud? Here, in this paper, we discuss how to secure data for cloud integrated Internet of Things. In two main steps we can ensure the data cannot be tampered. First, the CP-ABE (Cipher text Policy – Attribute Based Encryption) produces a secret key and encrypts the data. The data can only be decrypted when the secret key is correctly produced. The second way uses threshold cryptography where secret key is further encrypted by RSA and then generated key is divided internally and giving to a group of users. Shared key can be produced only if all the authorized users come together. Above proposed scheme not only provides confidentiality but also helps in reducing number of keys and prevents unauthorized/malicious users to access our data.

Keywords: CP-ABE (Cipher text Policy – Attribute Based Encryption), Threshold cryptography, Confidentiality, Malicious users.

I. INTRODUCTION

Cloud computing is well known for its storage. It makes easier to store and access data from any part around the world with the correct login credentials at any given time. We can also store massive amount of data on cloud. It is a Pay-as-you-go (PAYG) financial model which is reliable to all users and organizations. It provides good services such as Platform-as-a-service, Infrastructure-as-a-service and Software-as-a-service [9]. As we all use computers, iPods, mobiles etc., which we call internet of people, a new era of internet was developed which is internet of things where things communicate with things. For example, nest (Thermostat); it maintains temperature at our home by recording the initial temperatures that a person sets on a daily basis. It maintains the temperature and goes off when people are not around. In order to check and store the changes in the events we need storage.

Revised Manuscript Received on 8 February 2019.

Bingu Rajesh, Computer Science Engineering Department, KL University, City, Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India.

Puvvada Nagesh, Computer Science Engineering Department, KL University, City, Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India.

K Gowtham, Computer Science Engineering Department, KL University, City, Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India.

G Vivek, Computer Science Engineering Department, KL University, City, Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India.

N Srinivasu, Computer Science Engineering Department, KL University, City, Green Fields, Guntur District, Vaddeswaram, Andhra Pradesh, India.

This example is limited to a small set of people and therefore require a small storage but as population is more, large amount of data is being produced so where to store this huge amount of data? This is where cloud comes into the picture. So why don't we integrate cloud with IOT and store that massive data on cloud? Though cloud has many advantages it lacks in securing the data [9]. Although many preventive measures have been taken by cloud service providers (CSPs), the number of unauthorized users accessing the cloud is not less.

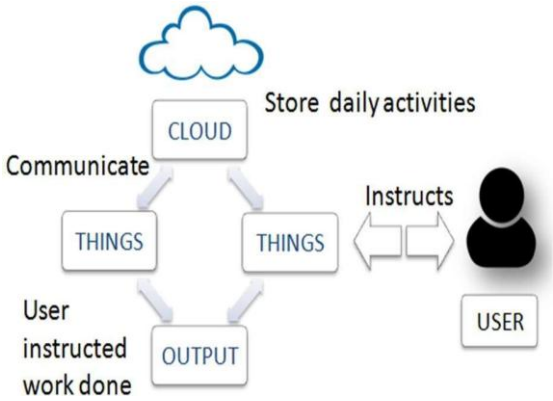

Fig 1. Cloud Integrated Internet of Thing

Therefore, after a survey, we propose a new scheme to secure cloud data which involve two stages for encryption. Firstly, with the help of public key and master key which is generated by KDC (Key distribution center) the CP-ABE produces a secret key and encrypts the data [1]. The data can be viewed only if the secret key generated is given correctly as input by the users [3]. In order to make the key more secure we can encrypt the key with threshold cryptography scheme [6] [8]. Where the key in internally encrypted with encryption algorithms like RSA, AES etc. and divided among the number of users [4]. Therefore, no unauthorized users can access data [10]. It is mandatory that all the internally divided keys must be present to retrieve the shared key. Hence, we can achieve confidentiality and it reduces the number of keys and unauthorized users. This paper contains 1. Brief Introduction about scheme, 2. Related work, 3. Existing model and assumptions, 3.1 Diagrammatic representation of algorithm, 4. Proposed scheme, 5. Results and Analysis of new scheme, 6. Conclusion and Future work, 7. Reference papers.

II. RELATED WORK

We have done a retrospective study. As Internet of Things need more space to store its data we are loading the data on cloud. Many schemes are proposed in this issue to store data produced by Internet of Things on cloud. As confidentiality plays a major role in this scenario, cloud is lagging to provide confidentiality and access control. The data sent to cloud by user is not secure [2]. Many new ways to encrypt data have been proposed to meet the requirements related to security issues but they failed in providing at most security. We have come across a new way to secure the data after obtaining the required information from recent studies in the standard journals. We have used CP-ABE as first encryption stage to generate a secret key by making use of the two keys generated by the KDC (trust worthy) [1]. In various journals they have used this CP-ABE it also encrypts the data and sends to the CSP. It has an Access policy 'A' in the attribute section. This algorithm gives SECRET KEY as an output. The cipher text message can only be decrypted when the user satisfies the following access policy and produce correct SK. We assume that cipher text implicitly has access policy 'A' [3]. This algorithm takes master key (MK) and attribute set 'S' as inputs. It generates a secret key (SK) with respect to attribute set S. This algorithm is appropriate for generating SK for shared information in fast growing industries; it can be applied to scenarios such as IOT [9].In the other part of encryption, we use threshold cryptography procedure [6] where an encrypted secret key using Deffie Hellman [3] is internally divided into several small chunks of keys based on the number of users. Instead of using 'N' number of keys for 'N' number of users. We can now reduce the number of keys to one per group. In order to decrypt the encrypted shared key all the requested key users (IOT maintenance team lead) must be present and only when all the small keys are combined we can get the whole entity of required encrypted secret key. Now the decrypted secret key is compared with the original Secret Key, once they are same the Data owner decrypts the data using CP-ABE decryption algorithm and produce the data to the users (IOT maintenance team).

The below table describes (Full Form) the abbreviations used in this paper.

Symbol	Description
MK	Master Key
SK	Secret Key
KDC	Key Distribution Center
CT	Cipher Text
CSP	Cloud Service Provider
M	Message
PK/PuK	Public Key
S	Set
DO	Data Owner
N	Number of users

From survey of previous papers [1] [4] [7] Totally, we have 4 main entities one is the KDC (key distribution center), DO (data owner), end Users (IOT team lead), and CSP's (cloud service providers).

Fig.2.Cypher text policy attribute-based algorithm (CP-ABE)

In CP-ABE the main concept is to generate a secret key and encrypt the data sent by the end user [1]. In return the DO sends a key (SK) to the user to access data in future. In order to get that key the DO requests KDC for the PK and MK then the KDC in return sends the two keys then the DO will generate SK [3].

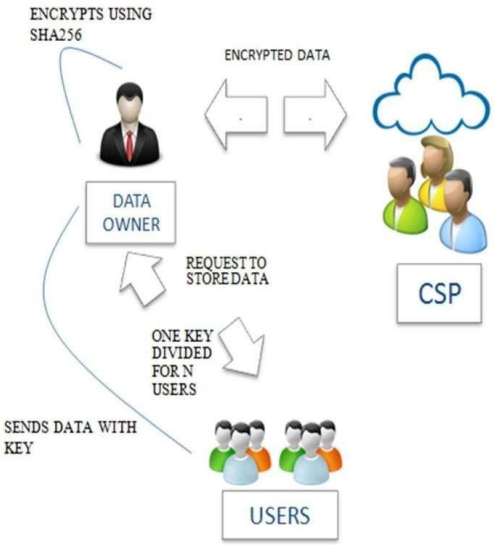

Fig.4.CP-ABE with Threshold scheme

In threshold cryptography the users first requests to store data. Then the Data Owner (DO) will divide a single key for 'N' users [5] and encrypts them with Deffie Hellman, SHA512 etc [4]. Encryption algorithm and sends the sub keys to users and send the encrypted data to CSP's(encrypt data using Deffie Hellman)[4].

III. PROPOSEDSCHEME

We propose an new scheme in the combination of CP- ABE and Threshold cryptography:

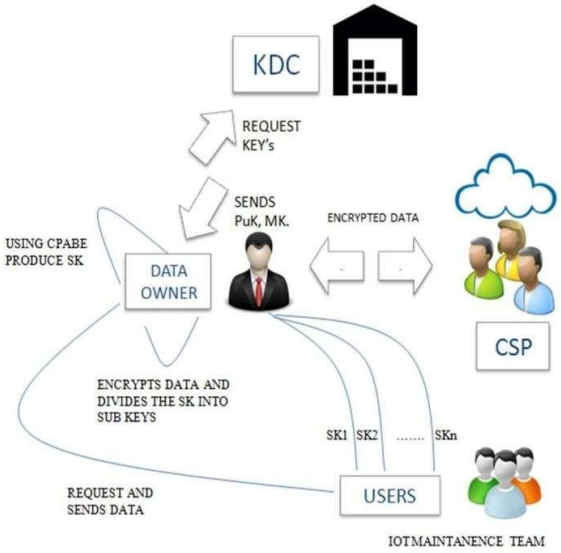

Fig.4.CP-ABE with Threshold scheme

All the data from IoT analysis is brought forward by the IoT maintenance people (Users)and they request the cloud to store the analyzed data. Therefore, we perform two stages to secure the data give by the users to cloudDO. At the first stage CP-ABE is associated to generate user's secret key and assess the access policy is related with attribute sets. It also encrypts the data and sends to CSP to store. In the process of users request for decryption, they can decrypt only when attributes satisfy the access policy included in cipher text and by producing the correct secret key generated before.CP-ABE engages only descriptive attributes excluding number of users and identities.
CP-ABE concludes the following fundamental basic algorithm

SETUP (^):

This algorithm takes public key parameter PK and Master Key MK from trust worthy as inputs.

ENCRYPT (PK, M, A): -

This function has following inputs Public key parameter PK, message M, and Access policy A in the attribute section. This function returns a cipher text CT. This cipher text can only be decrypted when the user satisfies the following access policy. We assume that cipher text implicitly has access policy A.

KEYGEN (MK, S): - This function takes master key MK and attributes set S as inputs. It generates secret key SK with respect to attribute set S.

DECRYPT (PK, CT, SK): - This function takes public key PK, cipher text CT and secret key SK as inputs. If the users' attribute set S satisfies the access structure'A'includedint the ciphertext CT, the nit decrypts the cipher text successfully and returns messageM.

After data sent to CSPtostoreinCloud, the secret key generated from above CPABE is now encrypted using RSA. Using Threshold cryptography, we internally divide the (RSA) encrypted SK among the 'N' number of users as SubKey1, SubKey2… Sub Key N. During decryption all the keys are combined together and decrypted combined key is taken by CP-ABE and data is produced.

ENCRYPTION

Encrypt the SK using the RSA algorithm.

Divide the encrypted SK among N Users SubKey1, SubKey2..Sub Key N.

Initialize an array size to n which contains default values null. On the base of acknowledgment from Usersuser1touserNupdatethevaluesInthearray to'1'.

DECRYPTION

Each user sends his sub key to the data owner.

If the Sub key is received by the DO he updates his respective value in array to '0' else'1'.

If all the keys are updated. He checks weather the array contains '1' if so he ack's the users that Secret key can't be generated.

Else if all the array values are updated and are0hecombinesthewholekeyandvalidateswith the Secret key (copy he has).If correct he decrypts the data by CPABE and allows the user to check his data. Else he ack's the users that Secret key can't be generated.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A. Diagramatic Representation Of Algorithm

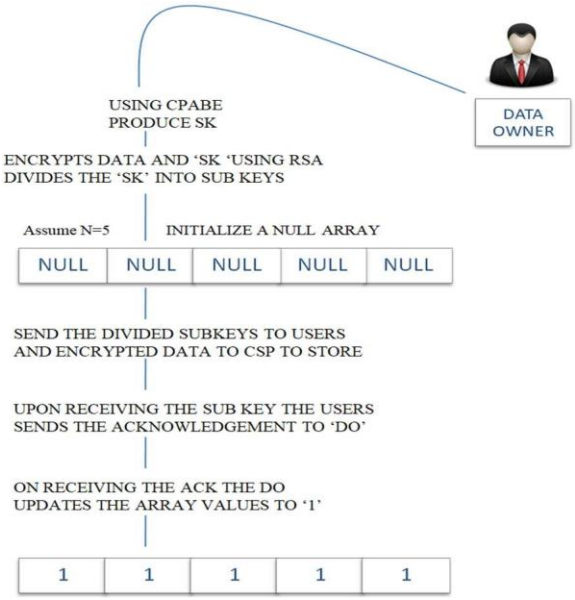

Fig.5. Encryption

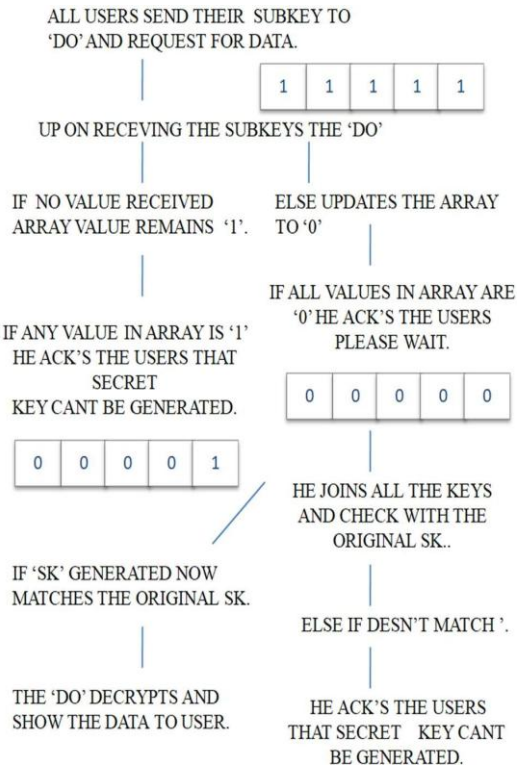

Fig.6. Decryption

IV. RESULT &ANALYSIS

Let us assume 'k' is the time taken to generate secret key using CP-ABE. Here 'k' increases with respective to attribute size. And time taken for encryption using secret key be 's' which includes encryption of data using CP-ABE.

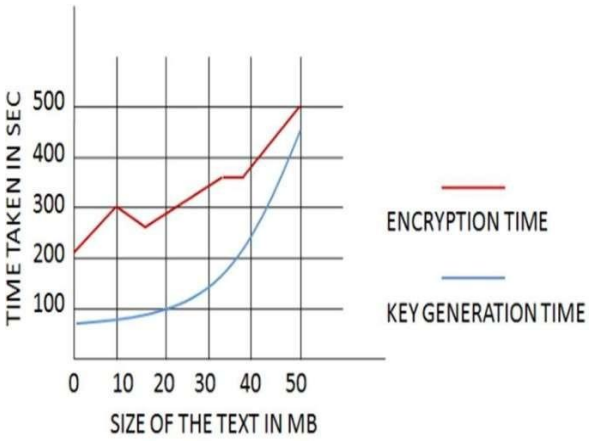

Fig.7. CP-ABE ANALYSIS

Now, time taken for encryption of secret key using RSA algorithm be 'n'.

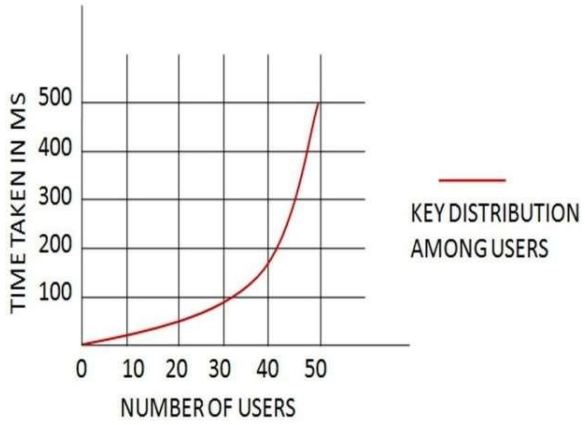

Fig 8.Threshold Analysis

Now this key is divided into m parts which takes 'x'(m=x) time where m is number of users. So, time taken over all key generation and encryption of text be 't'+'s'+'n'+'x'.

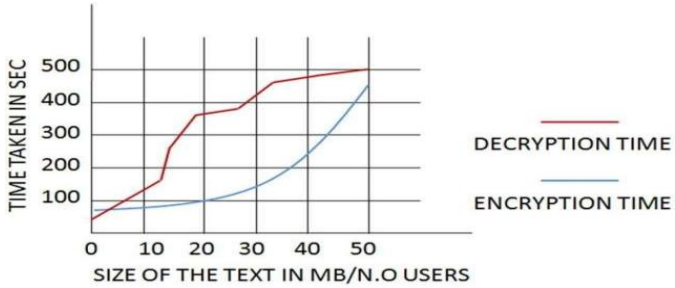

Fig9. Time for new scheme

The time taken for decryption is a bit slow when compared to encryption since decryption does much validation to achieve confidentiality for data and protect from unauthorized users. As IoT team checks the data (key authorization) in cloud once in a while time complexity is taken in a small scale.

V. CONCLUTION AND FUTUREWORK

As the users are increasing day by day work load on KDC is becoming more and more since it has to generate more number of keys for each user. We have a chance of collusion attack in order to suppress this we have come across this new scheme to achieve confidentiality. We used the threshold cryptography and CPABE scheme. We now use the above kind of encryption and store iot based data in cloud. Thus, it provides security for the iot data. My future work is to come up with new encryption techniques to safeguard the IOT based data in cloud.

ACKNOWLEDGMENT

We koppada.gowtham and gorantla. Vivek would like to thank our guide b rajesh for his keen interest and guidance throughout the project; and also p nagesh and n.srinivasu for their consistent support.

REFERENCES

1. Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian, and Jinguang Han, “Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing”, IEEE,2017.
2. Hongwei Li, Yuanshun Dai1, Ling Tian, “Identity based authentication for cloud computing”, Springer-Verlag Berlin Heidelberg.
3. Changji wang, Xuan Liu,Wentao Li,”Implementing a Personal Health Record Cloud Platform using Ciphertext-Policy Attribute Based Encryption”, International Confercne on Intelleigent Networking and Collaborative Systems.
4. Threshold cryptography-based data security in cloud computing. IEEE International Conferenceon Computational Intelligence & Communication Technology 2015.
5. A. Shamir. How to share a secret. Commun. ACM, 22, pp. 612-613, November 1979.
6. Ravleen Kaur, Pragya Kashmira, Kanak Meena, Dr. A.K.Mohapatra “Survey on Different Techniques of Threshold Cryptography”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).
7. Achieving efficient and secure data acquisition for cloud-supported IoT in smart grid, 2017 IEEE.
8. Secure Data Access in Cloud Computing, Sunil Sanka ,2010.
9. Jitender Grover1, Shikha 2, Mohit Sharma3, “Cloud Computing and Its Security Issues - A Review “, IEEE – 33044 , Dec 2015.
10. H. Zhong, and H. Zhen, An Efficient Authenticated Group Key Agreement Protocol,” Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, vol., no., pp.250-254, 8-11 Oct. 2007.

AUTHORS PROFILE

Bingu Rajesh received M.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Kakinada, India in 2012. He is currently working toward the PhD degree in the Computer Science from KL University, Guntur District, India. His research interest includes cloud IOT.

Puvvada Nagesh He is currently working toward the PhD degree in the Computer Science from KL University, Guntur District, India. His research interest includes cloud IOT.

Dr N Srinivasu, currently working as a Professor, Dept. of CSE, KL University, Guntur District, India. His research interest includes cloud .computing

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication