



## Enhanced Proficient System to Protect Data in Cloud Networking

Puvvada Nagesh<sup>1</sup>, N. Srinivasu<sup>2</sup>

<sup>1&2</sup> Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502.

pnagesh.qa@gmail.com , srinivasu28@kluniversity.in

### ABSTRACT

Many electronic gadgets/systems have become part of our daily life and they control many things, these things correspond with many other gadgets/systems around to complete the required task, this is IOT(Internet of Things). At present this would create huge data by IOT(Internet of Things). All this huge data can be stored in CLOUD. In this document we propose/discuss how the security can be provided for data in Cloud Networking Systems. We propose two important steps to ensure data is not hacked. In the first step, "Random Attribute Based Encryption" produce secret key and also encrypts data. For decrypting the data, secret key need to be accurate. In the second step, the key is again encrypted using RSA and the resultant key is made into recognizable pieces and shared among all the authorized persons. Secret key can be reproduced, if all the authorized users accept. The proposed system provides proficient mechanism and helps to stop hackers to fetch our data.

**Key words :** RABE (Random Attribute Based Encryption), Cryptography, Confidentiality, Hackers, Malicious users.

### 1. 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.

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.

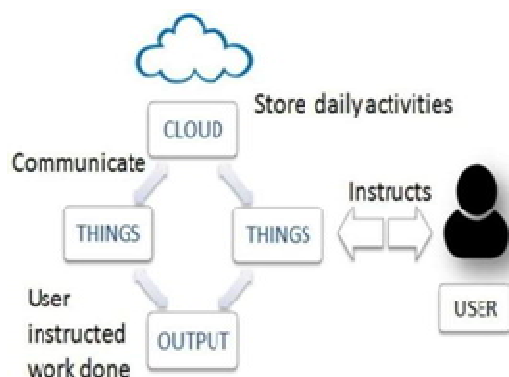


Figure 1: Cloud Integrated Internet of Thing

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 RABE 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 [10]. [8]. Where the key is internally encrypted with encryption algorithms like RSA, AES etc. and divided among the number of users [4]. Therefore, no unauthorized users can access data. 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.

### 2. 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 RABE 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 RABE 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 Diffie 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 RABE decryption algorithm and produce the data to the users (IOT maintenance team).

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

**Table 1:** The abbreviations used in this paper.

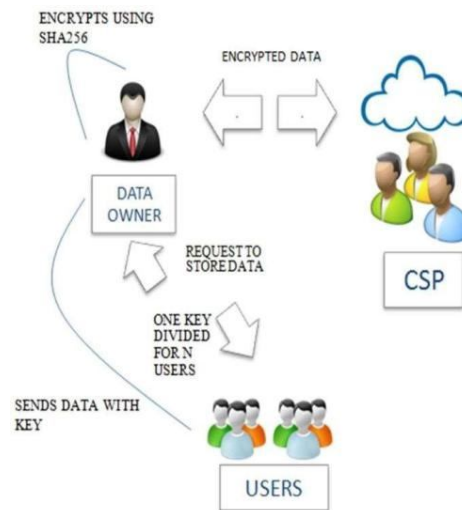
Symbol	Description
MK	Master Key
SK	Secret Key
KDC	Key Distribution Center
CT	Cipher Text
CSP	Cloud Service Provider
M	Message
PK/PuK	Public Key
S	Set
DO	Data Owner
N	Number of users

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).



**Figure 2:** Attribute-based algorithm (RABE)

In RABE 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].

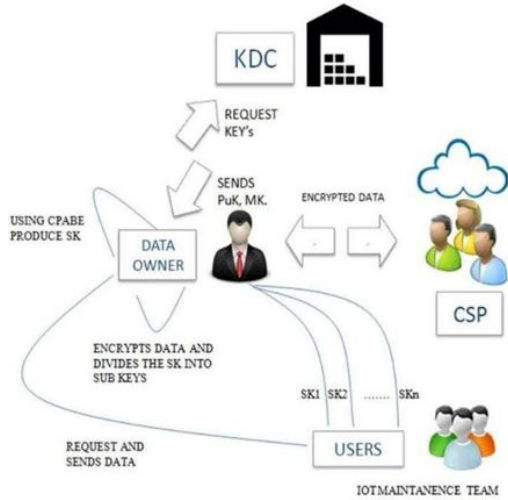


**Figure 3:** RABE with Threshold scheme

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 Diffie Hellman, SHA512 etc [4]. Encryption algorithm and sends the sub keys to users and send the encrypted data to CSP’s(encrypt data using Diffie Hellman)[4].

### 3 PROPOSED SCHEME

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



**Figure 4:** RABE 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 given by the users to cloud. At the first stage RABE 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. RABE engages only descriptive attributes excluding number of users and identities. RABE 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 user's attribute set S satisfies the access structure, A included in the ciphertext CT, the user decrypts the cipher text successfully and returns message M.

After data sent to CSP to store in Cloud, 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 RABE 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 User user I to user N update the values in the array to „1“.

**DECRYPTION**

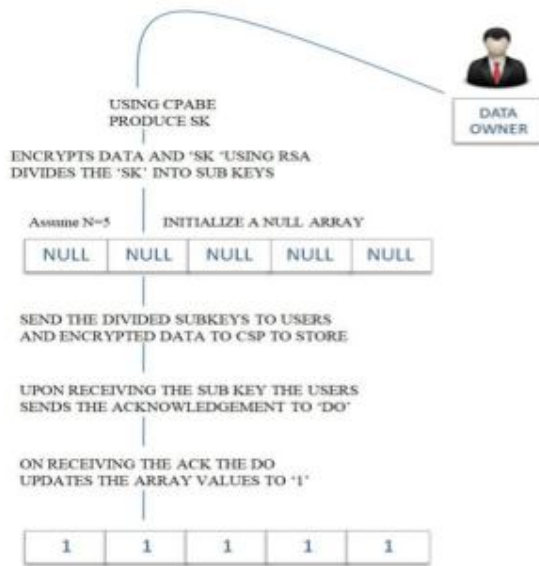
Each user sends his sub key to the data owner.

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

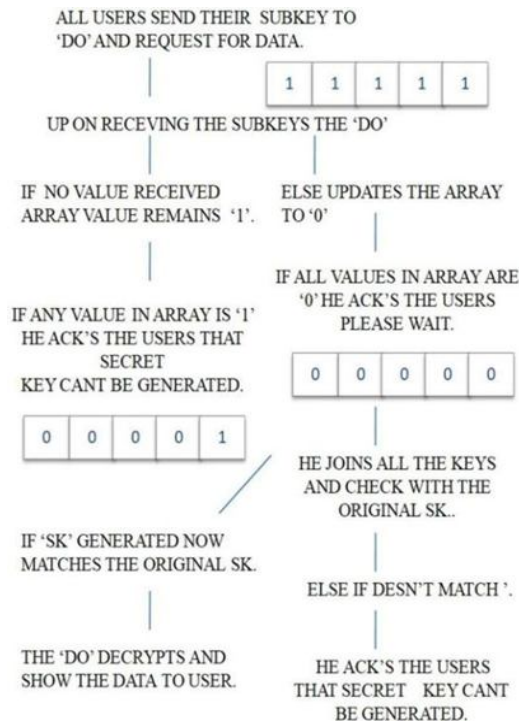
If all the keys are updated. He checks whether the array contains „1“ if so he acknowledges the users that Secret key can't be generated.

Else if all the array values are updated and are 0 he combines the whole key and validates with the Secret key (copy he has). If correct he decrypts the data by CPABE and allows the user to check his data. Else he acknowledges the users that Secret key can't be generated.

### 2.1 Diagrammatic Representation Of Algorithm



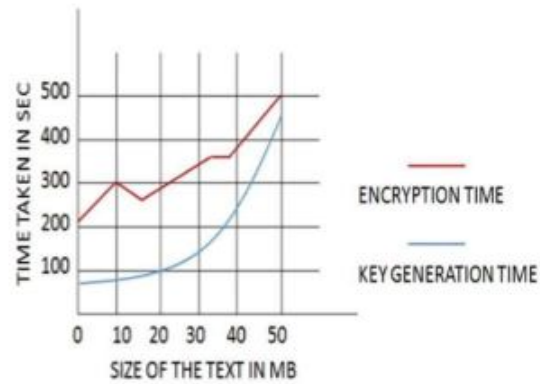
**FIGURE 5: ENCRYPTION**



**Figure 6: Decryption**

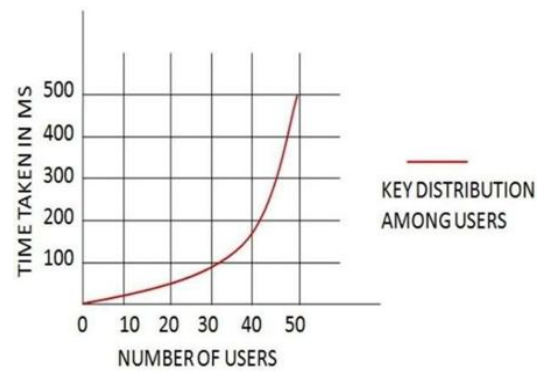
### 4. RESULT & ANALYSIS

Let us assume „k“ is the time taken to generate secret key using RABE. Here „k“ increases with respective to attribute size. And time taken for encryption using secret key be “s” which includes encryption of data using RABE.



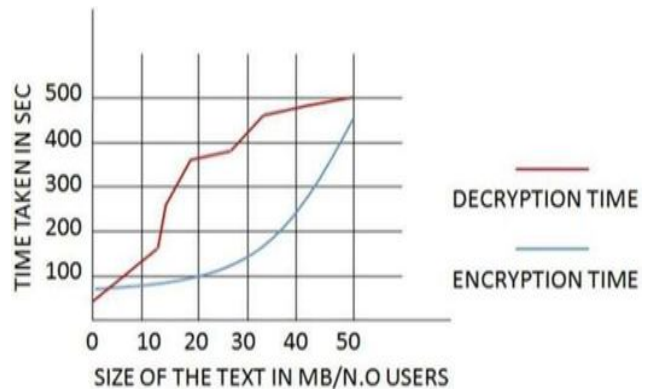
**FIGURE 7: RABE ANALYSIS**

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



**Figure 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“.



**Figure 9: 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.

## 5. CONCLUSION 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.

## 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 Dai, 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 Conference on Intelligent Networking and Collaborative Systems.
4. **Threshold cryptography-based data security in cloud computing.** IEEE International Conference on Computational Intelligence & Communication Technology 2015.
5. Pree et al. **Design patterns of object oriented software development Reading**, Mass.: Addison-wesley, 1995
6. Aizu Keitsiro, **Possible species of ferromagnetic, ferroelectric and ferroelastic crystal**, Phys. Rev. B, 2, 754-772,1970.
7. Nagesh, P., Radha Madhavi, M., Surendra Prasad Babu, M. **Reusable object oriented design for stereographic projections of tetragonal point groups**, International Journal of Innovative Technology and Exploring Engineering, volume.8,No.8,177-180,2019.
8. Lanka, S., Madhavi.M.R., Abusahmin, B. S., Puvvada, N., & Lakshminarayana, V., **Predictive data mining techniques for management of high dimensional big-data**, *Journal of Industrial Pollution Control*, 33, 1430-1436,2017.
9. Ramesh Babu, A., Radha Madhavi, M., Sarala, S., & Lakshminarayana, V., **Tensor pairs and domain pairs of cesium dihydrogen phosphate using group theoretical techniques.** *Journal of Industrial Pollution Control*, 33, 1475-1480,2017.
10. Madhavi, R., Karri, R. R., Sankar, D. S., Nagesh, P., & Lakshminarayana, V., **Nature inspired techniques to solve complex engineering problems.** *Journal of Industrial Pollution Control*, 33(1), 1304-1311,2017.
11. Puvvada, N., & Prasad Babu, M. S. **Semantic web based banana expert system.** International Journal of Mechanical and Production Engineering Research and Development, 8(3), 364-371,2018.

12. Venkata Ramana, N., Nagesh, P., Lanka, S., & Karri, R. R. , **Big data analytics and iot gadgets for tech savvy cities.** doi:10.1007/978-3-030-03302-6\_12,2019.
13. Venkata Ramana, N., Seravana Kumar, P. V. M., & Nagesh, P., **Analytic architecture to overcome real time traffic control as an intelligent transportation system using big data.** International Journal of Engineering and Technology(UAE), 7(2.18 Special Issue 18), 7-11,2018.
14. Venkata Ramana, N., Nagesh, P., Seravana Kumar, P. V. M., & Vignesh, U. **IoT based scientific design to conquer constant movement control as a canny transportation framework utilizing huge information available in cloud networks.** Journal of Advanced Research in Dynamical and Control Systems, 10(7 Special Issue), 1395-1402,2018.
15. Rajesh, B., Nagesh, P., Gowtham, K., Vivek, G., & Srinivasu, N. **A new scheme to safeguard data for cloud integrated internet things,** International Journal of Innovative Technology and Exploring Engineering, 8(4), 174-178,2019.
16. Venkata Ramana, N., Kolli, C. S., Ravi Kumar, T., & Nagesh, P. . **Hybrid K-mir algorithm to predict type of lung cancer among stoicism.** International Journal of Innovative Technology and Exploring Engineering, 8(4), 283-287,2019.
17. G Siva Nageswara Rao.et al. **Efficient PIMRR Algorithm for Improving scheduling Criteria’s in Real Time Systems,** International Journal of Engineering and Technology (ISSN 2227-524X) volume 7, No. 2.32, Special Issue 32, pp 275-278, July. 2018.
18. G Siva Nageswara Rao.et al. **Modern Vehicle Tracking and Monitoring System using Embedded Technology,** International Journal of Recent Technology and Engineering (IJRTE) (ISSN 2277-3878) volume 8, Issue 1, pp 1849-1851, May 2019.
19. G Siva Nageswara Rao.et al. **Food Waste Protein sequence analysis using clustering and classification techniques,** International Journal of Advanced trends in computer science and Engineering (ISSN 2278-3091) volume 8, Issue 5, pp 2289-2298, October 2019.
20. Vijaya, N., Madhavi, M. R.,et al., **Boundary layer of a mixed convective nanofluid flowing over a vertical circular cylinder under the influence of magnetic field, heat radiation and outside surface temperature.** International Journal of Mechanical and Production Engineering Research and Development, 8, pp. 411-420, 2018.
21. Gobinath Ravindra, M. Radha Madhavi **Optimization of Zinc(II) Adsorption Using Agricultural Waste,** International Journal of Engineering & Technology, 7 (3.34) ,300-304,2018.