Available online at http://www.ijims.com

ISSN - (Print): 2519 – 7908 ; ISSN - (Electronic): 2348 – 0343

IF:4.335; Index Copernicus (IC) Value: 60.59; Peer-reviewed Journal

Data Encryption using SCT and access control using TRBAC in Cloud Computing for Big Data

Akhilesh Dwivedi[1*], R P Pant [2], Martand Pande[3]

1.Deptt of CSE, Graphic Era Hill University, Bhimtal

2. Deptt of Mathematic, DSB Campus, Kumaon University

3. Free Lancer

*Corresponding author: Akhilesh Dwivedi

Abstract

Cloud Computing is the emerging trend to process different types of data and provide different services, and Big data is the huge source of such data. In this paper we proposed a framework in which we encrypt data with clock timing and then provide access according to task and role of the user. By this we can achieve a full secured and authorized access to cloud user with secure big data user.

Keywords- Big data, cloud computing, RBAC, Task, SCT encryption

I. Introduction

Cloud Computing provides many services to different consumers or users without any necessity of deep knowledge of the technology. To provide such services, one need to secure system such that only legitimate user can access such services. And on the other side, one needs some data set to collaborate with the service provided by cloud service provider. For such huge data, we have a term called Big Data which mean to store huge data, analyze that data for various purposes such as for business purposes, for curing diseases and many others [12, 13, 14, 16, 17]. In this paper, we propose a framework in which owner encrypt its data with Clock timing (SCT) described in [11] when it storing data to cloud storage, and when user try to access data then it must have permission according to its task and role [15] Section II briefs about cloud computing, Section III explains about Big data and section IV, discusses security aspects of big data, Section V, and VI throws light on TRBAC and SCT respectively and Sec VII , explains proposed framework, and section VIII concludes this paper.

II. Cloud Computing

Cloud means something away from one place; here cloud refers to network or internet. User's system is connected by network which is away from user's system and contains pool of resources, and these resources used by user of cloud provider. Cloud Computing is emerging technology which provide easy and affordable services [1]. The three basic components of cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [1] as shown in fig 1.

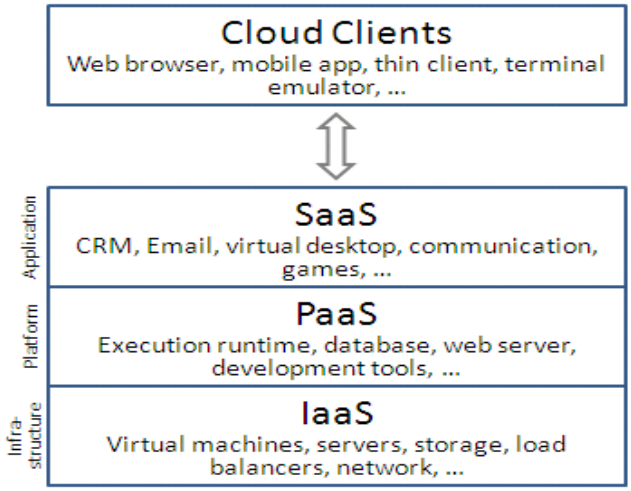

Fig.1. Architecture of Cloud Computing

III. Big Data

Big Data is a collection of complex or too large data, which is difficult to handle by traditional data base mechanism. As it is difficult to handle but also it benefit a lot in many other ways.

The Big data can be described basically in two types of system. System for capture and stored data and the other type is systems that provide analysis capabilities of the data that has been stored. The main challenge is to data storage, data analysis. Data analysis can correlate with the Business trends and curing disease. It is a connection of 3V that is volume, velocity and variety.

IV. Security Of Big Data

The main challenge in Big Data is query processing on encrypted data. And nowadays both type of data structured or unstructured need decryption first which is quite slow. The traditional system of data encryption and decryption consist data query generation on encrypted data then decrypt by using private key then result generation by query processing and then at last data encryption by using public key.

V. Task-Role Based Access Control Model (Trbac) For Cloud Data

The idea to use **Task-Role Based Access Control** (TRBAC) **[4, 15]** is to extract the task and role to be two basic characteristics for cloud based data access. This model appoints task to role, then appoints permission to task described in detail in [15]. To realize permission dynamically, the connection of permission and task is important, but the purpose of role and task connection is to carry out of related information between task and object. As described in [11, 15], when the permission of role updates, using task as resonance is convenient for the role management. Fig 2 shows the basic model of TRBAC [11, 15], which has four major components Task Set, Role Set, User Set and Session Set. There are few four important definitions of these sets of TRABC model briefly explained as below. The detailed functioning of TRBAC model is explained in [15], however, we explained it in brief here.

Defination 1. *User Set* $U = \{u_1, u_2, \ldots u_n\}$ is the user set of different users, including personal user, departmental user and so on.

Defination 2. *Session Set* $S = \{s_1, s2, \ldots s_n\}$ is the session set. The Role is activated based on session.in the browser by user.

Defination 3. *Role Set* $R = \{r_1, r_2 \ldots r_n\}$ *is the role set.* The Role of a person is according to position in the organization.

Defination 4. *Task Set* $T = \{t_1, t2, \ldots, t_n\}$ is the task set. The Task is the basic unit of the TRABC model, according to task; role is assigned to the user.

VI. The Data Encryption Using Substitution Clock And Its' Time (SCT)

Figure 3 shows the basic functionality of SCT [11]. The SCT algorithm works on the concept of analog clocks' Time [11]. This algorithm can encrypt 8-bits of data at a time.

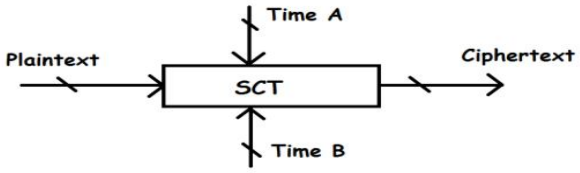

Fig.3. Basic working diagram of SCT [11]

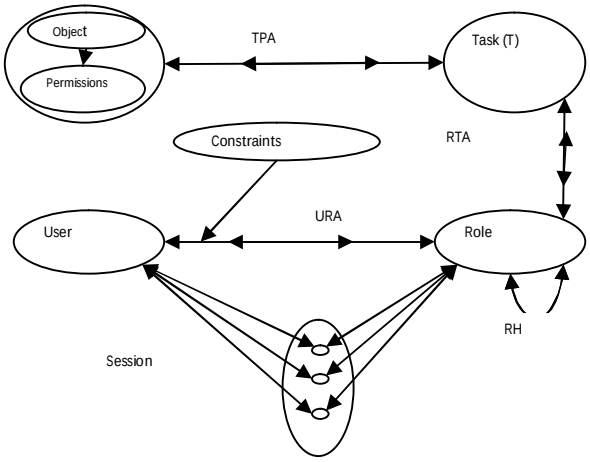

Fig.2. Fundamental model of TRBAC, which consist of Task, Role, User and Session

Various components of SCT are explained below.

A. Time A

First component, this is the time noted in the first action of the user that's why it is called as Time A. For example, at the time of opening a page of cloud website, or a cloud application, or the time before input of the plaintext.

B. Time B

Second Component, this is the time noted in the second action that's why it is called as Time B. For example, Login into a website, time after plaintext was entered.

Let's take an example: Suppose someone opened a website (Example: Google drive). The time at which he opened the website will be time A. And the time at which he will login to a website after entering information will be time B. The information he entered will be treated as plaintext. The terminologies used in SCT algorithm [11] are briefly discussed below:

i. Encryption Layer (EL)
ii. Substitution Clock (S-Clock)
iii. Encryption Time (ET)
iv. Encryption Time Values (ETV)
v. Random Operation Array (ROA)
vi. Random Operation Function (ROF)

i. Encryption Layer (EL)

The Encryption layer is just a combination of random distribution of 256 numbers (0 to 255) mapped over an analog clock. So SCT used this layer beyond the normal clock but based on normal clocks' appearance.

ii. Substitution Clock (S-Clock)

The Substitution Clock used in SCT is of the size 12 (in terms of hours) as there are 12 hours (1-12) mentioned in this clock. This means there are 12 positions to represent a number of hours in a clock [11].

iii. Encryption Time (ET)

In the SCT, first of all, time A and time B will be passed to the SCT time function [11]. This time function will take the values of time A and time B and will return a random time. This generated time will be a random time between time A and time B. This time will be mapped on s-clock and is known as encryption time (ET).

iv. Encryption Time Value (ETV)

ETV is the value which we got from s-clock at a particular time by user behaviour. This is of 3 bits based on 3 values (hours, min, and sec) from clock reading.

v. Random Operation Array (ROA)

It is an array which will select 8 operations out of 10 to be performed in the plaintext bytes. Every byte will undergo one out of the selected 8 operations [11] and repetitions of process will be in cyclic manner.

Example: ROA = [7, 8, 10, 1, 3, 2, 6, 5]

The 7^{th} operation will be performed on 1^{st} byte. The 8^{th} operation will be performed on 2^{nd} byte. In the same way, the 9^{th} byte will undergo a 7^{th} operation in a cyclic manner.

vi. Random Operation Function (ROF)

This is a function which will take 8-bit (one byte) as an input, perform any one of the 10 operations in those 8-bit and returns one position of the s-clock. It will be decided randomly by ROA whether which operation will be done on those 8-bits.

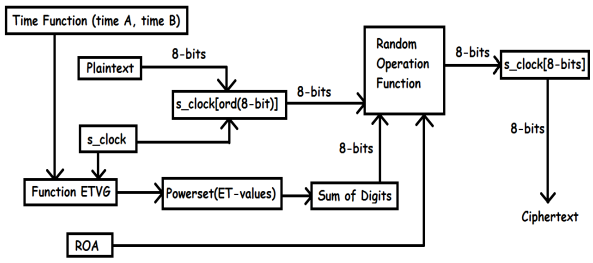

Fig.4. Complete working of SCT [11]

The complete working of SCT is shown fig 4 as per [11] and we have developed algorithm for SCT in [11] and implemented and tested using python. Detailed discussion on security analysis and comparison with AES is performed in [11] and shown below in fig 5 less time consumption while execution.

Fig.5. Time taken for encryption and decryption by SCT [11]

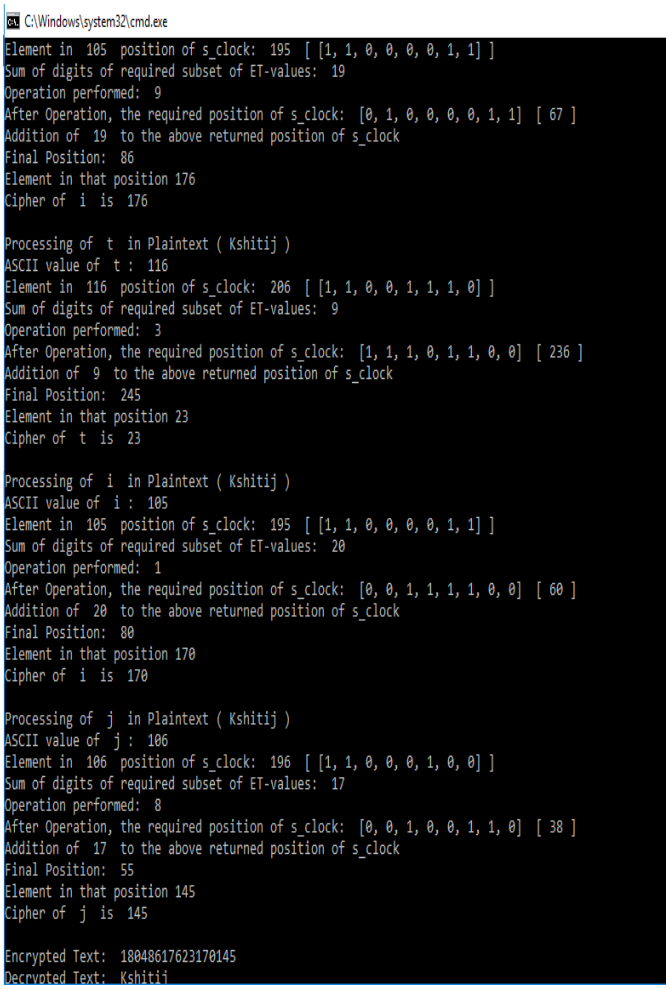

Fig.6. Execution of SCT algorithm in python

VII. Proposed Framework

The fig 6 shows implementation of SCT in python for cloud and big data storage. See below the basic process flow diagram of framework proposed method in fig 7, as we know Cloud Computing is one the important part of our day to day life, it provide

so many services to make our life easy. As it provide so many services, so as to have data storage and processing task too. So to store such data, cloud has a large storage system such as big data, and to secure such data from unauthorized users and several attacks, cloud have so many algorithms to encrypt data and also have so many access control policies to control access from unauthorized user. Figure 7 shows the working of proposed model.

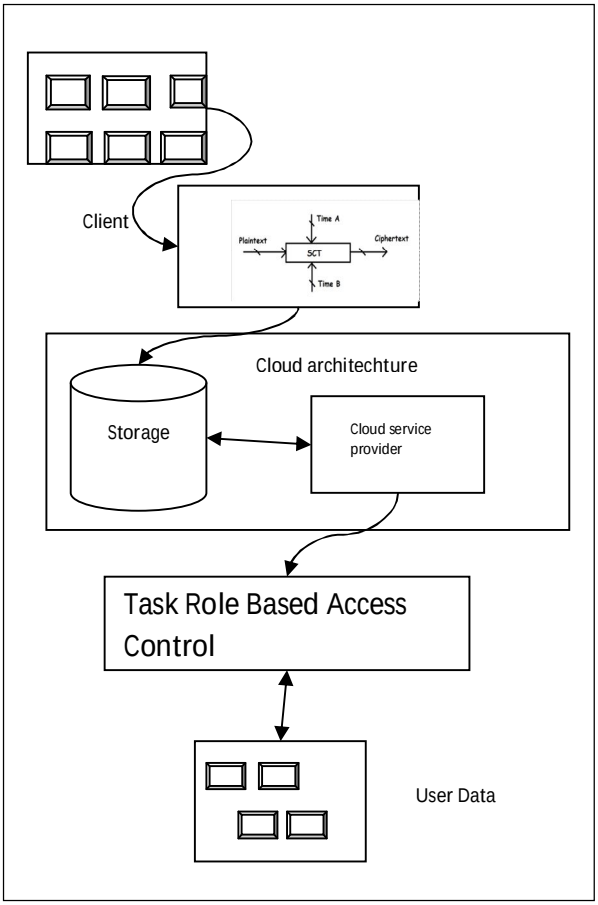

Fig.7. Proposed framework for data encryption and decryption

VIII. Conclusion

In this paper we proposed a model which encrypt data with clock timing and then provide access according to task and role of the user. We found our proposed approach is faster than AES. AES has a key combination of 2^{256} ($2^{256}=10^{77}$) and SCT and TRBAC algorithm has an s-clock combination of 10^{506} [7, 11]. By this we can achieve a secure environment for stored data and no unauthorized user can access data until that user have permitted task and role then after this that user must have private key to decrypt the stored data which encrypted by data owner according to SCT encryption method. This framework can be extended with other algorithms to generate hybrid encryption technique that is used for security and privacy for email, IoT and cloud and big data storage [11, 12, 13, 14, 15, 16, 17]. This proposed model is secured in terms of access control and encryption mechanism.

References

[1] Eeva Savolainen, “Cloud Service Models”, UNIVERSITY OF HELSINKI.

[2] Natarajan Meghanathan, Lynch St,Jackson “REVIEW OF ACCESS CONTROL MODELS FOR CLOUD COMPUTING”, Jackson State University,, USA.

[3] Singh et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(6) June - 2013,pp. 1136-1142
IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.7B, July 2006

[4] Ganglidis Antonios, Mavridis Loannis,”Towards new access control model for cloud computing system” University of macedonio,Greece.

[5] K-Y. Chen, C-Y. Lin and T-W. Hou, "The Low-Cost Secure Sessions of Access Control Model for Distributed Applications by Public Personal Smart Cards," Proceedings of the 17th IEEE International Conference on Parallel and Distributed Systems, pp. 894-899, December 2011.

[6] Young-Gi Min1), Hyo-Jin Shin2), Young-Hwan" "Cloud Computing Security Issues and Access Control Solutions"

[7] E. Bertino, P. A. Bonatti and E. Ferrari, "TRBAC: A Temporal Role-based Access Control Model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191-233, August 2001.

[8] J. B. D. Joshi, E. Bertino, U. Latif and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model," IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 1, pp. 4-23, January 2005.

[9] C. L. Dumitrescu and I. Foster, "GRUBER: A Grid Resource Usage SLA Broker," Euro-Par 2005, LNCS 3648, pp. 465-474, 2005.

[10] Liu Sainan, "Task-role-based access control model and its implementation" by College of Publish HangzhouDianziUniversity"

[11] Dwivedi Akhilesh, K Kala, J Pant, RP Pant, Senam Pandey, Vertika Kandpal, "A Novice Encryption Technique using Substitution Clock and Time in It (SCT)" 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN) 2018, 23- 24 Feb. 2018 Year: Pages: 1 - 6, DOI: 10.1109/ICACCAF.2016.7748991

[12] J Pant, A Juyal, H Pant, A Dwivedi, "A Real-Time Application of Soft Set in Parameterization Reduction for Decision Making Problem", International Journal of Electrical and Computer Engineering (IJECE), 2017/2/1, Volume 7, Issue 1, Pages 324-329

[13] Krishna Kumar and Akhilesh Dwivedi, "Big Data Issues and Challenges in 21st Century", International Journal of Emerging Technologies (Special Issue NCETST-2017), Volume 8, Issue 1, Pages 72-77

[14] Priyanka Suyal, Janmejay Pant, Akhilesh Dwivedi, Manoj Chandra Lohani, "Performance evaluation of rough set based classification models to intrusion detection system", Advances in Computing, Communication, & Automation (ICACCA)(Fall), IEEE International Conference, 2016/9/30, 1-6

[15] Senam Pandey, Akhilesh Dwivedi, Janmejay Pant, Manoj Lohani, "Security enforcement using TRBAC in cloud computing", Computing, Communication and Automation (ICCCA), 2016 IEEE International Conference, 2016/4/29,1232-1238

[16] Akhilesh Dwivedi, Abhishek Dwivedi, Suresh Kumar, Satish Kumar Pandey, Priyanka Dabra, "A cryptographic algorithm analysis for security threats of Semantic E-Commerce Web (SECW) for electronic payment transaction system" Advances in Computing and Information Technology,2013, Springer Berlin Heidelberg, Pages 367-379

[17] Dwivedi Akhilesh, RP Pant, S Pandey, K Kumar, "Internet of Things' (IoT's) Impact on Decision Oriented Applications of Big Data Sentiment Analysis" 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU 2018), Pages: 1232 - 1238, DOI: 10.1109/CCAA.2016.7813905