International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Data Secure Algorithm in Cloud Storage

T. Senthil Kumaran , A. Muruganandham, M.Mathivanan

Abstract: ***The challenging task is protecting the data which are uploaded to the cloud becomes bigger worries in a cloud environment system. In this type of security is needed for monitoring of data access in a cloud environment and is getting more and more attention in recent days. Few strategies which can be afford for top-secret and an unknown authentication for delicate information and it is more efficient than doing the encrypting data first and then sign or doing the sign first then encrypting the data. However, in so many previous work, delicate information of data users can be reveal to authority, and only the authority is responsible to answer to that type of attribute management and generation of key in the system. The proposed system states that confidentiality and protective of data access control over the cipher text scheme based on cloud security. It is provide a control measure, attribute confidentiality and guard the data's of user concurrently in a multiple authority cloud system. Both the attributes of designcryptor and signcryptor can be kept secret by not knowing to the authorities and cloud storage server. Besides, decryption in the clouds for users as becomes meaningfully reduced by outsourcing the unwanted bilinear pairing process to the cloud server without humiliating the attribute privacy. The planned scheme is confirmed for protecting the standard model and has the skill to provide top secret, unforged, unknown authentication, and verifiability of public. The security analysis which are relating to comparison of difficulty and results of execution will indicate that the proposed system has the capacity to balance the security issues with respect to computation in hypothetical efficiency.***

Keywords :. Security, Encryption

I. INTRODUCTION

In this world, there is quick growth in field of cloud environment and lot of users are prefers to store the bulk of data in cloud storage system with respect to price effective way [1, 6]. Taking into consideration all this aspects of profits by the cloud server, protecting the data accessing is become one of the most risky task for us meanwhile cloud storage is not completely trust worthy for the data users while accessing of data which are stored in cloud storage might be having delicate information of users. Henceforth, protecting the privacy of users and making the data secrecy by not making public, first data user needs to encrypt the information which they want to store in the cloud storage system [2]. Delicate information are viewed in point of the data user can share the information with different users, but user should assure for some attributes.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
T. Senthilkumaran, Department of CSE, ACS College of Engineering Bangalore, India.
A. Muruganandhan*, Department of ECE, Rajarajeswari College of Engineering, Bangalore, India.
M. Mathivanan, Department of ECE, ACS College of Engineering, Bangalore, India.

So now to advance the system storage and computation of storage, PHR facility may provide the support for TTP cloud system to data storing. Data which are in PHR system may contain delicate information [3].
It should be assured that only the data user like the doctor who is handling the patient has the freedom to access the data information of patient. Let me take one example of data user of name xyz which uploads the personal record of health issues to the server (here server means cloud server), so by this cloud server it may checked that data of users with certain identification such as gender age (between 20 and 30) [4]. When a hospital named "xxx" may contact the information which are loaded in personal health record system, so doctor can confirm that this type of data may belong to xxx / age fits to range of '20 to 30' but the most important thing is that users (or patient) original id information 'xyz' is kept top secret[5].

II. LITERATURE SURVEY

Cloud computing symbolizes today's best thrilling computing concept shift in information technology. In this survey noted again, security and privacy are observed as primary obstacles to its wide assumption. Here, the creator plan several serious security challenges and inspire further study of security solutions for a truthful public cloud environment. In this work we have discussed several serious security challenges that current research points aren't so for addressing [1].

Author presents a KP-ABE architecture with fixed size cipher texts, whose security is verified under the decisional linear (DLIN) standard model. The access structure is expressive, easy to read and also has an easy encryption. In Decryption only a linear pairing option is present. They also suggest a secret key which is secure and continuous. In specific, several algebraic properties of a decoratively chosen sparse matrix group are applied to the dual system security evidences. In this system they are improving security but communication overhead[2].

It presenting an open key cryptography environment, joint encryption and signature systems have smart characteristics and they are occasionally used. The combine security of encryption has a history which is wide. This Scheme is proposed and focused on a key is known as Joined public key. They are proposed a architecture for CP-ABE and ABS models. A secure model of ABS is based on waters model. This model is selectively secure; they also give the suggestions on how to construct an ABSC Model[3].

ABSC can achieve the functionality of ABS and ABE logically. Both are separated into two types: 1) KP (Key Policy) and 2) Cp (Cipher Policy). In this scheme they presented an ABSC and this is the first ABSC policy called as hybrid policy.

They Presented KCP-ABSC Architecture has ability to choose attacks a cipher texts models. The size is constant in the KCP-ABSC model. i.e. The attributes used in the system is independent[4].

III. SYSTEM MODEL

The authorities and securities can be viewed in the following ways

***CA*:** It also called as Global Certificate Authority; it can produce the public activity for the system by execution global setup algorithm. It is also answerable for authorities' registration and data users. Throughout the process, it can confirm the id of the valid authority and user.

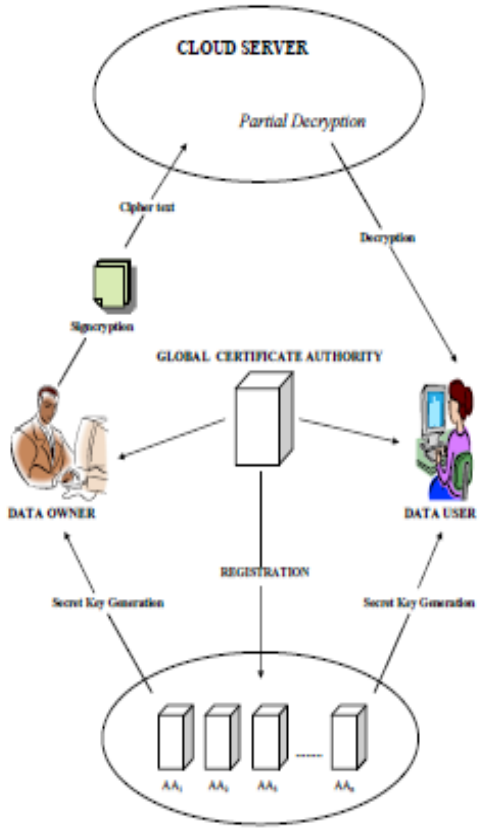

Fig :1 working Model.

AA: It can prepare own setup. its secret key and public key using authority algorithm setup. To determine the users by SK, authorities confirms the user id and to run SK generation to create the SK. SK generations algorithm can be more expand to improve a SK generation algorithm to keep the attribute confidentiality.

A. Cloud server

It is answerable to loading of delicate data file upload by the data user. The Cloud sever can too complementary accessed to user. Meanwhile our system maintenance take the confirmation by public and it can confirm that the cipher text is workable or not, then attribute fulfil, the sign based limited in the cipher text from signcrypted by the data user. The CS can discard it, when the cipher text is not effective. Also it is execute the incomplete decryption algorithm to support the user decrypt of the cipher text with users changed SK.

B. Signcryptor

Signcryptor also called as a data owner. When the data user signcrypts the text, user can select the encryption with signing for all authority and outsources the output of cipher text to the cloud server by succession signcryption algorithm. Following correct output of the cipher text is to follow it, in signing the attributes must please signing bases. We undertake the cipher text indirectly comprises encrypt and signing founds. Only valid exist user can approve the data and the predicates can decrypt the data filled by only user.

C. Designcryptor

This designcryptor is also called as data user throughout the signcryption phase, to enter the subtle data, attribute decryption must be performed by the user and must fulfil the data owner from encrypted predicates specified. The data user is continuously resources limit: we work on 2 methods, to efficiency of the user. The public confirmation is the first method. To check the strength and reliability of the cipher text from any reliable 3rd party used by data user, and don't need to make confirmation on his individual device. The outsourced decrypted deprived of humiliating the attribute confidentiality. The efficiency of decryption algorithm can enhance on the side of data user.

D. METHODOLOGIES

AES encryption algorithm is used for both encryption and decryption of data. The secret key generation algorithm is used to generate the secret key for data users. All having a chunk size of 128 bits, according to this AES,it has three different key chunk sizes: 128, 192 and 256 bits. As all know that AES is best for encryption and decryption, this is the best algorithm when compare to other algorithms because it is much secured.Recently added user with uid wants to appeal a authority AAJ to secret key, AAj confirms the users certainly (uid) with confirmation key vkCA. If it's legal user, AAj executes the secret key generation algorithm defined as follow the user by generate the secret key.

IV. RESULTS

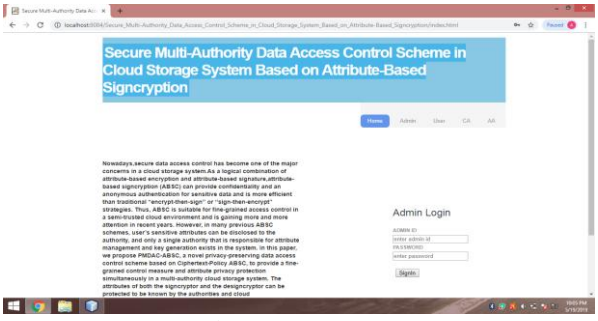

Fig:2 Home page

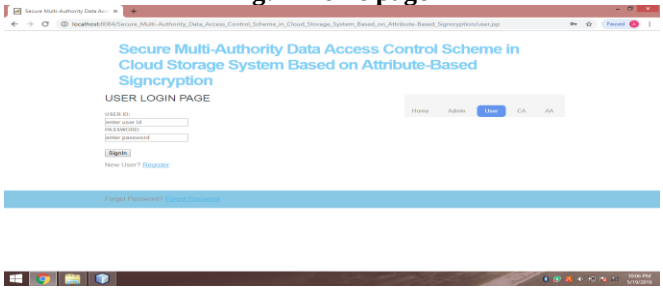

Fig:3 User Login page

Fig:4 User File Uploading with Signcryption.

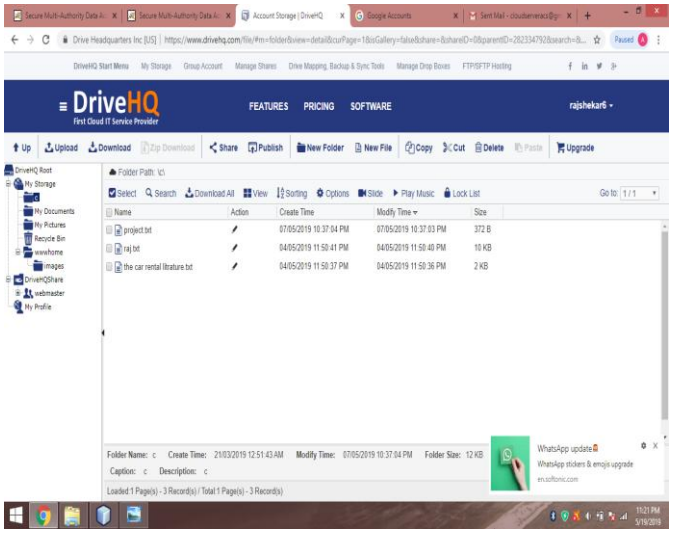

Fig :7 Files Stored in Cloud Server.

Fig:5Files Uploaded by User to Cloud Server.

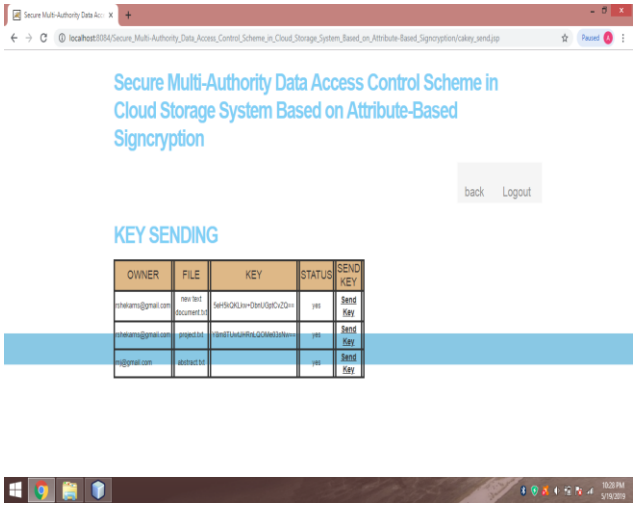

Fig: 8 Sending Secret Key.

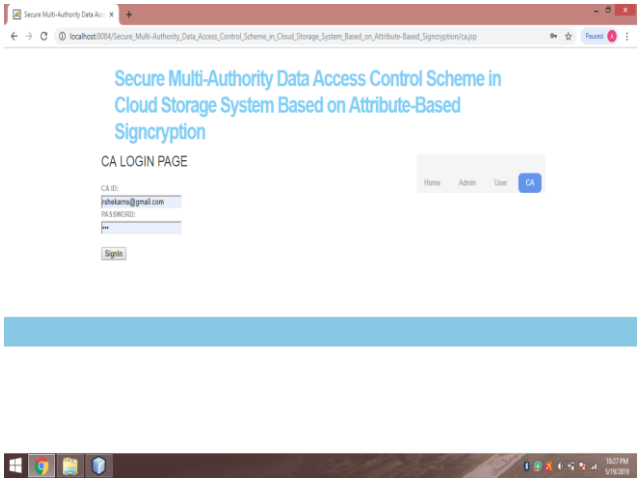

Fig: 6 CA Login Page.

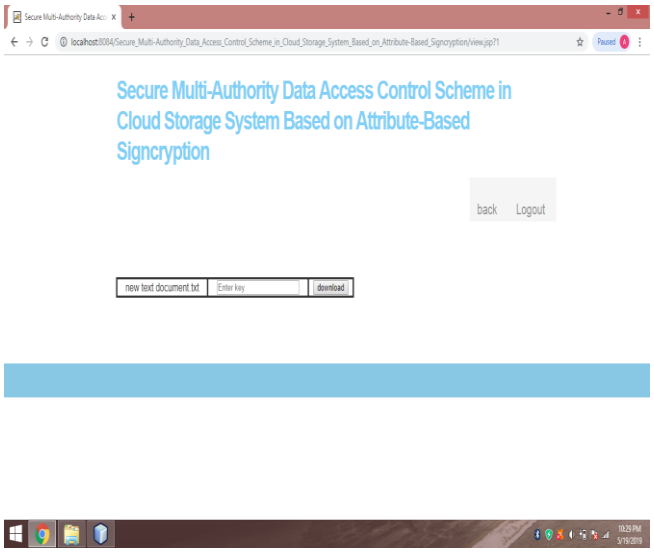

Fig 9: Downloading File by Entering Secret Key.

The Figure 2-9 is proven that the secret key algorithm id out performed and successfully provides security in cloud environment

V. CONCLUSION

This algorithm presents Privacy Preserving Multiple Authority Data Access Control of cloud server and uploading the data in cloud storage system while protecting the users attributes. In this architecture multiple Attribute Authorities can issue the key for users and they work independently. The secret key is send by the Attribute Authorities to the users without knowing their Attributes. Comparing the performances and the Security parameters, this scheme can manage the security and can balance the overhead efficiency. Because of the expensive operations the privacy of the attribute is degraded in the cloud server is managed. In the future a secured system can be realized, in addition to that how overhead storage can be decreased by providing the similar levels of security is another task.

REFERENCES

1. P. Mell and T. Grance, ‘‘The NIST definition of cloud computing,’’ Commun. ACM, vol. 53, no. 6, pp. 50–53, 2010.
2. S. Kamara and K. Lauter, ‘‘Cryptographic cloud storage,’’ in Proc. 14th Int. Conf. Financial Cryptogr. Data Secur., Tenerife, Spain, Jan. 2010, pp. 136–149.
3. K. Maji, M. Prabhakaran, and M. Rosulek, ‘‘Attribute-based signatures,’’ in Topics in Cryptology—CT-RSA. Berlin, Germany: Springer, Feb. 2011, pp. 376–392.
4. K.Ren,C.Wang,and Q.Wang,‘‘Security challenges for the public cloud,’’ IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan. 2012.
5. M. Gagné, S. Narayan, and R. Safavi-Naini, ‘‘Threshold attributebased signcryption,’’ in Security and Cryptography for Networks. Berlin, Germany: Springer, Sep. 2010, pp. 154–171.
6. Y. S. Rao and R. Dutta, ‘‘Expressive attribute based signcryption with constant-size ciphertext,’’ in Progress in Cryptology—AFRICACRYPT. Cham, Switzerland: Springer, May 2014, pp. 398–419.

AUTHORS PROFILE

Dr T. Senthil Kumaran received Doctoral Degree, 2014. He has got teaching, research and administrative experience of more than 18 years in various engineering colleges, autonomous institutions and universities. He has published more than 20 papers in national and international conferences and in international journals.. He is a Life member of the ISTE, Senior Member IACSIT, Life Member IAENG, Member ICST, IAES

Dr. A. Muruganandham received Ph.D (Image Compression) in the year 2013, He is a life member of ISTE, Fiend member of IEEE. He has a teaching experience of 23 years. His-research interests includes Image processing and Bio Medical Engineering.

Dr. M. Mathivanan received Ph.D 2014, Chennai. He has 18 years of teaching experience and more than 10 years of research experience. He has published 10 research articles in International Journals and more than 10 National & International Conferences. He is the life time member of ISTE and IETE professional societies.