Secured Cloud Data Transmission using Cross ABE Algorithm

K. Chockalingam, L. Velmurugan

Abstract*: Cloud security is becoming more essential than ever with the tremendous development of delicate cloud data. The cloud information and services are located in massively scalable data centers and can be accessed anywhere. Unfortunately, the development of cloud users has been followed by an increase in cloud malicious activity. More and more vulnerabilities are being found, and fresh safety advisories are being released almost every day. Millions of customers surf the cloud for different reasons, so they need extremely secure and persistent services. The cloud storage system interconnect with the a load of potential security risks. So the cross encryption of Ciphertext Policy Attribute Based Encryption (CPAB) and Key Policy Attribute-based encryption algorithm which increases the security level in the encryption side. A segmentation part helps in splitting the encrypted file in storing the data in the cloud side, the Desegmentation part in the receiver side can easily combines spitted data into the single file for validation examine an authentication level in the received data. Here the cloud storage easily with the file fragmentation processes. This processes research over the storing mass amount of data on off- site installation, which can eliminate the cost in maintaining the physical hardware. Cloud's future includes a much greater degree of privacy and authentication, particularly in extending the variety of apps. We suggest a straightforward data protection model where data is encrypted before it is introduced in the cloud using key policy attribute-based encryption to ensure data confidentiality and safety. The storing data is the most common application for the cloud server.

Keywords: Cloud computing, Attribute based Encryption, privacy, Security.

I. INTRODUCTION

Cloud computing technology is the use of computing resources supplied through a network as a service. Users need to provide access to their data in the cloud computing system to store and play the company activities defined. Cloud service provider should therefore give confidence and safety, as precious and sensitive data is kept on the clouds in big quantities. In cloud computing, there are problems related to versatile, climbable and fine grained access management. There are several schemes scheduled for coding for this purpose. Like the simple method of coding that has been researched classically. We tend to discuss attribute-based coding (ABE) systems and how they were created and altered to Key Policy Attribute mainly based coding (KP-ABE), Cipher-text Policy Attribute mainly based coding (CP-ABE) and additionally scheduled as CP-ASBE and thus HABE and HASBE. However flexible, climbable and fine-grained access management is given by each theme, this can be compatible.

II. RELATED WORK

KaitaiLiang *et al.*, [9] are proposing the main cloud-based rescindable identity-based proxy re-encoding (CR-IB-PRE) theme that promotes user revocation but joint delegation of decoding privileges. Despite the user being revoked or not, the cloud acting as a proxy may re-encrypt all user ciphertexts below this period of time to the following period of time at the top of a given period of time. If the user is cancelled within the next period of time, the invalid non-public key will no longer be able to rewrite the ciphertexts by mistreatment. We tend to point out that this primitive applies to a number of sensitive network applications, such as subscription-based cloud storage Services Examination of some naive alternatives requiring a private key generator (PKG) to behave at any time with unrevoked users, the fresh theme offers definite blessings in terms of communication and computing efficiency. Our theme only needs the PKG to publish a public string of constant size for each period of time, and the work of updating ciphertexts is loaded onto the cloud server. Much considerably, in the normal model, the theme is tested securely. YounghoPark *et al*[10] offer a fully safe CP-ABE scheme with a non-monotonic access structure for a large region of attributes. Our scheme achieves absolute safe definition by providing a symptom that no polynomial time wrongdoer can differentiate the allocation in a very true game and a final game by the twin secret writing framework for mistreatment. The competitor gets a semi-functional type two version of secret key or ciphertext continuously in the final match. This means that the competitor cannot, with queried secret key, generate decipherment to the challenge ciphertext that embodies individuals who meet the access structure of the challenge. In addition to AND, OR and threshold gates that add the ex-pressibility access management, our theme allows users to jointly outline NO doors within the access tree. Our CP-ABE gift scheme jointly allows for huge universe attributes as the overall public parameter within the CP-ABE gift does not grow linearly with region size attributes.

Revised Manuscript Received on February 05, 2020.
* Correspondence Author

K. Chockalingam,*Department of Computer Science, Research Scholar, Joseph Arts and Science College, Thirunavalur, India. Email: Palaniappanshiva7@gmail.com

Dr. L. Velmurugan, Department of Computer Science, Assistant Professor, Joseph Arts & Science College, Thirunavalur , India. Email: apcpksona@gmail.com

Retrieval Number: C5149029320/2020©BEIESP
DOI: 10.35940/ijeat.C5149.029320
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

What's more, our scheduled CP-ABE can be used in real-world applications from memory demand and computing cost analysis. Joseph K. Liu *et al* [11] addresses the open drawback of suggesting an escape resilience secret writing model that captures escape from each main owner (data user or management center) and thus the encrypted (data owner or sensor) in the auxiliary input model. We tend to fix this disadvantage by processing the post-challenge auxiliary input model in which the escape function family should be described before the overall public key is offered to the person. The post-challenge issue may return to the escape from the encryptor's use of secret writing randomness. This model is capable of capturing a wider real-world attack category. Yanjiangrule *et al* [12] granted associate degree expanded proxy-assisted strategy in order to overcome the restriction of cloud server confidence that proxy keys intrinsic in proxy / mediator-assisted user revocation methods are not disclosed to customers .In our approach, we tend to bind the non-public key of the cloud server to the operation of information decipherment, which requires the cloud server to reveal its non-public key. We tend to develop a primitive,' revocable encryption of cloud data' underneath the strategy. We tend to give concrete building to the primitive and use the proof-of-concept to enforce growth. The experimental findings suggested that our building be suitable even on sensitive mobile devices for preparing. Willy Susilo *et al* [13] scheduled a message will be encrypted { in a associate degree exceedingly a very } ciphertext linked to a capricious length index string, and a decryptor will be valid if the string is accepted and provided by a DFA associated to its secret key.What's more, a semitrusted proxy to whom a re-encryption key is provided allows the greater than secret writing to be changed to a distinct ciphertext linked to a brand new string.The proxy, however, cannot achieve access to the plaintext underlying it. This fresh primitive will make consumers more flexible in delegating their freedoms of decipherment to others. Within the normal model, we tend to demonstrate it jointly as totally selected-ciphertext secure.

III. ISSUES IN CLOUD COMPUTING SECURITY

Data security is one of the safety problems addressed by [4] in cloud computing. Any technology is a prevalent problem, but when Software-as - a-service (SaaS) consumers have to depend on their suppliers for adequate security [9-11] it becomes a significant challenge. In other words, safety leaks are the primary problem in cloud computing, preventing individuals from fully embracing cloud technologies. Since all documents are stored in the cloud servers and are always available, hackers have full-time working hours to crack file safety walls such as encryption and authentication. Below are the safety problems that have been mentioned in cloud service suppliers and are directly linked to file storage.

A.Secure data Transfer

Cloud computing is about networking that has a real-time channel of communication with customers to send and receive data packets. These information packages, however, can be readily monitored as the web is used for interaction and at any moment susceptible to assaults. The cloud computing service suppliers must therefore ensure that the files or portion of the data file are correctly protected for complete security.

B.Secure data Storage

Clouds store enormous amounts of user information. For some parties, some of the stored data may be extremely important. Cloud services need to be very well integrated with data encryption and decryption to create client confidence. Data is encrypted and stored in cloud servers in all recognized cloud services. The decryption key is implemented when the user requests to view the information to decrypt the information and then display it by the customers. This type of file encryption and decryption is used to safeguard unauthorized user access to cloud servers

C.User permissions

The accessibility constraints of users over files and records of other users are another safety factor in cloud computing. When providing the right login credentials, a user is authenticated in the server. Users are not allowed to access personal or non-public files uploaded by other users, however. Users should be aware of who has management privileges in cloud service suppliers for data management reasons because they have the power to access information stored in clouds

IV. PROBLEM SOLUTION

To tackle the above cloud security problems effectively, we need to know the safety of the compound. In a holistic manner, the challenges. In particular, we must: I explore multiple cloud safety characteristics, including vulnerabilities, threats, hazards, and models of attack; (ii) identify safety criteria, including confidentiality, integrity, accessibility, transparency, etc.; (iii) define the parties concerned (customers, service providers, outsiders, insiders) and the role of each party in the process of attack-defense; (iv) understanding the effect of safety on different models of cloud deployment (public, community, personal, hybrid).
The primary input of this article is a safe encryption system for sharing encrypted information between a set of approved users and achieving effective user revocation for unreliable clouds. Security in cloud computing is a significant element of service quality. In order to maintain the delicate user data confidential against untrusted servers, several encryption techniques are used. Cross-ABE (Key-Policy Attribute based encryption) encryption system has been suggested based on the trusted authority that leverages the efficiency needed for encryption functions within the cloud itself. A trusted authority is solely accountable for important regeneration, which results in more effective and scalable safety. We suggest a cloud-based safe data system that enables trusted authorities to safely store their secret information on semi-trusted cloud service suppliers and selectively share their secret information with a broad spectrum of information receivers to decrease the key management complexity of authority holders and information receivers. Differentiation from prior cloud-based data system, information holders uses the cross-ABE encryption scheme to encrypt their secret information for information receivers. After encryption, the information is divided into 6 components and stored in the cloud (information centers) in a distinct division. Another sophisticated specification is to send the application to the authority (information proprietor) if any information receiver wants to download private file.

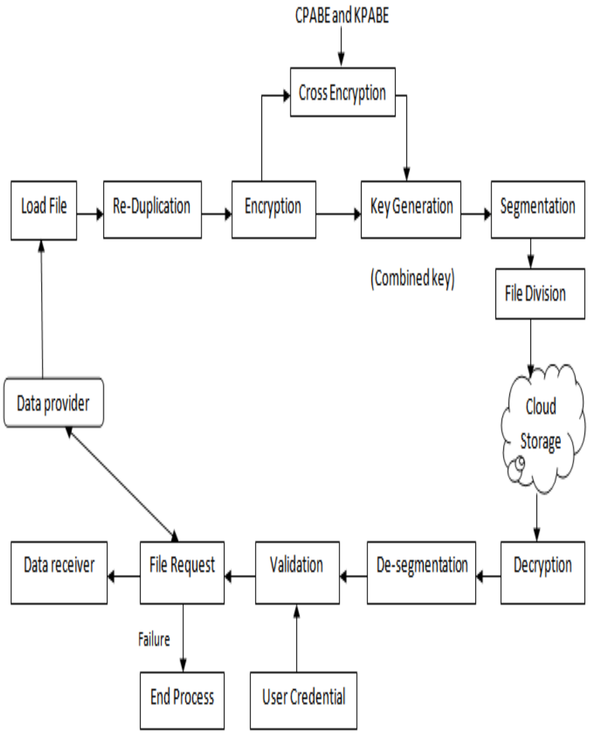

Fig. 1. Proposed System Model

The Fig.1. shows the proprietor of the power has the control of access. If the Owner wishes to share the initial file with the information receiver, the application will be accepted otherwise the application will be refused by the information proprietor. After the application has been accepted, the information receiver downloads the keys and this key is primarily for validation and downloading in the initial format (decrypted format).

V. SYSTEM MODEL

A. Global Setup

This algorithm takes as outputs the system parameters paramsandinput a security parameter *l*.

B. Data Owner Setup

(*SKi, PKi, Di*).Each Owner Di(automatic) generates his secret and public key pair KG *(1l) (SKi; PKi)* and an access structure *Di*, for i=1,2; . . .N.

C. Encryption

This algorithm takes as input the system parameters params, a message M and a set of attributes *DC*, and outputs the cipher text CT, where *Dc={ Dc1,Dc2.....DcN} ˜Dci ∩ Di.*

D. Segmentation

This algorithm takes as input the system parameters params, a message M and a set of attributes *DC*, and outputs the cipher text CT in to 6 parts DC1,DC2…..DC6, where *Dc={ Dc1,Dc2.....DcN} ˜Dci ∩ Di*

E. Key generation

Each Owner Di takes as input his secret key SKi, a global identifier GID and a set of attributes *Di* GID, and outputs the secret keys *SKiU*, where *DiGID = DGID ∩Di ,DGID* and *Di* denote the attributes corresponding to the GID and monitored by Di, respectively.

F. Desegmentation

This algorithm takes the inputs of PKi,Ski and verifies where *Dc={ Dc1,Dc2.....DcN} ˜Dci ∩ Di thn*DC1,DC2…..DC6 to message M.

G. Decryption: This algorithm takes as input a GID the secret keys cipher text CT and outputs the message M, where *Ic*is the index set of the authorities *Di* such that *Aic≠{ }*

VI. RESULT AND DISCUSSION

Table 1: Number of random key generation and the encryption and decryption method[13] .

Sl.No.	Key Generation	Encryption	Decryption
1	152	1.06	1.08
2	138	1.02	0.98
3	154	1.01	1.01
4	174	0.9	1.02
5	145	0.65	0.6
6	183	1.02	1.03
7	143	0.99	1.04

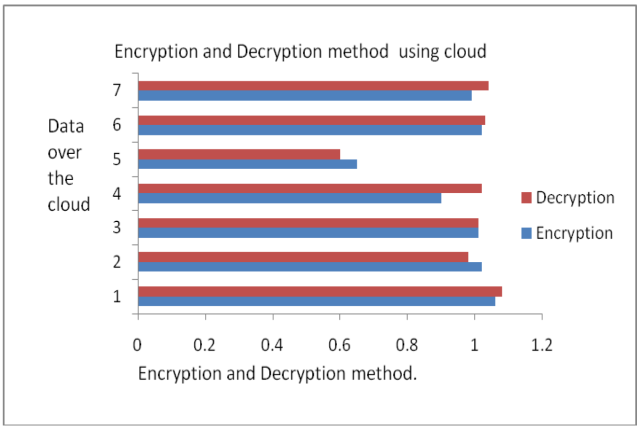

Fig. 2. Encryption and Decryption in cloud[13].

The figure 2 shows the encryption and decryption percentage in cloud for various number of keys. The encryption decryption properly used in the cloud storage method using the secured key distribution.

VII. CONCLUSION

Cloud computing is a mixture of a number of main techniques evolving and maturing over the years. Cloud computing offers businesses a potential for cost savings, but there is also a huge security risk. The security risk of cloud computing should be seriously analyzed by enterprises looking at cloud computing technology as a manner to cut costs and boost profitability. Cloud computing power in data risk management is the capacity from a centralized level to handle risk more efficiently.

While cloud computing can be seen as a fresh phenomenon set to revolutionize how we use the Internet, there's a lot to be careful about. Many new technologies are emerging at a fast pace, each with advances in technology and the ability to make life simpler for humans.

The frame work concluded over the security risk level reduces the combination of both the Ciphertext Policy Attribute Based Encryption (CPAB) and Key Policy Attribute-based encryption algorithm. However, to comprehend the safety hazards and difficulties presented by the use of these techniques, one must be very cautious. There is no exception to cloud computing. Key safety factors and difficulties presently facing cloud computing are outlined in this article. In encouraging a safe, virtual and economically feasible IT solution in the future, cloud computing has the ability to become a leader.

REFERENCES

1. K.Yang and J.Xiaohua, “Security for Cloud Storage Systems”, Springer temporary in applied science, 2014.
2. T. Chou, “Security Threats on Cloud Computing Vulnerabilities,” International Journal of applied science Technology, vol. 5(3), pp. 79–88, 2013.
3. J. Strickland, “How Cloud Computing Works,” Howstuffworks.com. Retrieved from http://computer.howstuffworks.com/cloudcomputing.htm, 2011.
4. K.Hashizume, D.G. Rosado, E. Fernandez-Medina, and E.B. Fernandez, “An analysis of security problems for cloud computing,” Journal of web Services and Application, 4:5, Feb 2013.
5. Beckham, the highest 5 security risks of cloud computing, out there on internet: http://blogs.cisco.com/smallbusiness/the-top-5-securityrisks-of-cloud-computing, 2011.
6. F. Kerby, , “Understanding coding,” The Monthly Security Awareness write up for pc Users, The SANS Institute, Editorial Board: B. Wyman, W. Scrivens, P.Hoffman, L.Spitzner, C.R. Hardy , July 2011.
7. Alanazi, H. O., Zaidan, B. B., Zaidan, a. a., Jalab, H. a., Shabbir, M., & Al-Nabhani Y, “New Comparative Study Between DES, 3DES and AES among 9 Factors,” Journal of Computing, vol. 2(3), 152–157, Mare 2010.
8. E. Milanov , “The RSA formula,” pp. 1–11, June 2009.
9. JW. Rittinghouse and JF Ransome, “Security within the Cloud,” In: Cloud Computing. Implementation, Management, and Security, CRC Press, 2009.
10. S. Subashini and V.Kavitha, “A survey on Security problems in commission delivery models of Cloud Computing,” Journal Network and pc Applications, vol. 34(1), pp. 1-11, 2011.
11. J Viega, “Cloud Computing and also the common person,” Journal pc vol. 42(8), pp. 106-108, Aug 2009.
12. P.K. Pagadala and J.Sabeena, "Enhancing the protection and reliableness of the information over pc Networks victimisation RSA cryptosystem," Int. Journal of Innovative analysis in Technology," vol. 1(6), pp. 195- 202, 2014.
13. Dr A.M. Gonsai and L.M. Raval, "Evaluation of Common coding formula and Scope of Advanced formula for Simulated Wireless Network,", Int. Journal of pc Trends and Technology, vol.11(1), pp. 7-12, May 2014.

AUTHORS PROFILE

Mr. K. Chockalingam, M.Sc., M.Phil., (Ph.D.), ADGMS., Completed post graduate with distinction from Thiruvalluvar University. Completed M.Phil. With distinction from Thiruvalluvar University. Currently doing Ph.D., - Thiruvalluvar University. Completed ADGMS (Advance diploma in graphics multimedia suite). Attended multiple national &amp;international seminars &amp; symposiums. Resource person for Microsoft MAC’s academy. Resource person for CPGS&amp;co teaching and technical solutions. Visiting guest faculty at Arts and Engineering colleges.

Dr. L. Velmurugan, Department of Computer Science, Assistant Professor, Joseph Arts & Science College, Thirunavalur , India. Email: apcpksona@gmail.com

.