ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Securely Sharing Critical Information in Cloud Environment Using Mediated Certificateless Encryption System.

Bosubabu Sambana
M.Tech(CSE)
Sarada Institute of Science, Technology And Management,
Srikakulam, Andhra Pradesh.

Mula Sudhakar
Assistant Professor
Sarada Institute of Science, Technology And Management,
Srikakulam, Andhra Pradesh.

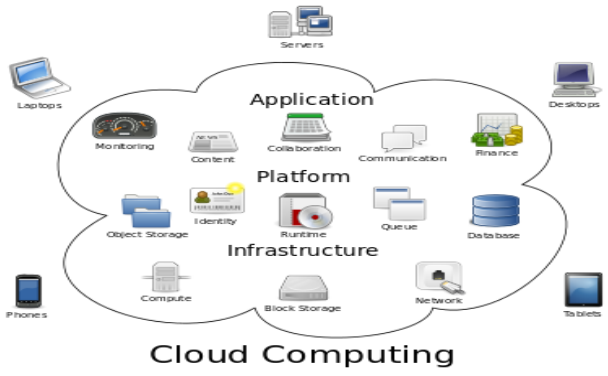
Abstract:
Now a day's public cloud storages are more benefits for provide service to users for manage their data. However for the rapidly increase of public cloud storage, the public cloud should solve the major issue of data confidentiality. That is sharing sensitive data through all the data must be strongly secured for unauthorized access. In order to provide security of sensitive data store in public clouds, a commonly used approach is to encrypt data before upload into public clouds. So that to provide confidentiality of stored public cloud data, the encryption mechanism isshould also able to support to access confidential data. In this paper we are propose public key encryption schema for generation of secret key and encrypt the data using that key. The generation of secret key we are using publickey power auditing protocol. Another concept is encryption and decryption of data using data encryption standard algorithm. By implementing those concepts we can improve efficiency and security of give shared data in a cloud.

Keywords: ***Encryption, cloud computing, Symmetric key, Information security.***

Introduction:

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

But security issue is most significant concern to protect data in the cloud. The concerns of data security are growing because the existing progress of the internet and the simplicity of data delivery and communication. Data safety is serious in every aspects of our lives; banking information, private documents and businesses. Nearly all of those are processed with technologies and all through network communication. A very essential cause safety concerns are raising is as companies are running core and non-core business functions from side to side other companies. To guarantee confidentiality of responsive data stored in public cloud; a frequently adopted scheme is to encrypt data previously to uploading it to the cloud. As the cloud does not see the keys used to encrypt the data, the privacy of the data as of the cloud is protected. Cryptography is the procedure of achieving security by encrypting/encoding data to make them non-readable, the method of encoding plain text messages into cipher text messages is called as Encryption, there are a number of methods to encrypt the data. Encryption of the data is the way to defend the data from malevolent and not permitted users, encryption of the data can be more than one level, and several levels of the encryption improve the security of the data but increase the encryption charge for the owner. So, there are a number of scheme to care for the data items, and 'Encryption of the Data' is one of them.

Two kinds of encryption system is used in cryptography i) Symmetric key, ii) Asymmetric key. To encrypt/decrypt the data secret or public/private key is used, in symmetric key approach single key is used to encrypt and decrypt the data but in asymmetric key approach dissimilar keys are used to encrypt and decrypt the data. Symmetric key technique is quicker than asymmetric key technique in encryption and decryption of the data. But asymmetric key system is better than symmetric key in security, key management & distribution standpoint. Asymmetric key is accepted for security of the data since asymmetric key system provides more protection than symmetric key system. This paper proposes the certification of the users and revocation of the malevolent users, revocation of the spiteful users is very much important to defend the data from malicious use; for that cause in this system cloud does revocation of the malevolent users and it is set for the aim that registration of the users. In symmetric key system

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

secret key must be kept private and this key only accessible for two mutual users but in asymmetric key system it is not necessary of the public key to be kept confidential because public key is used to show anyone who gives data to the private key owner. There are several symmetric key algorithms, Blowfish is used for fast encryption/decryption of data and it is symmetric key method thus there is no need of maintaining the public and private key both.

Existing System:

Due to the benefits of public cloud storage, organizationshave been adopting public cloud services such asMicrosoft SkyDrive andDrop box to manage theirdata. However, for the widespread adoption of cloud storageservices, the public cloud storage model should solvethe critical issue of data confidentiality. That is, shared sensitivedata must be strongly secured from unauthorizedaccesses. In order to assure confidentiality of sensitive datastored in public clouds, a commonly adopted approachis to encrypt the data before uploading it to the cloud.Since the cloud does not know the keys used to encryptthe data, the confidentiality of the data from the cloud isassured. However, as many organizations are required toenforce fine-grained access control to the data, the encryptionmechanism should also be able to support fine-grainedencryption based access control. As shown in Fig. 1, a typicalapproach used to support fine-grained encryption basedaccess control is to encrypt different sets of data items towhich the same access control policy applies with differentsymmetric keys and give users either the relevant keys or the ability to derive the keys. Even thoughthe key derivation-based approaches reduce the number ofkeys to be managed, symmetric key based mechanisms ingeneral have the problem of high costs for key management.In order to reduce the overhead of key management, and an alternative is to use a public key cryptosystem. However,a traditional public key cryptosystem requires a trustedCertificate Authority (CA) to issue digital certificates thatbind users to their public keys. Because the CA has togenerate its own signature on each user's public key andmanage each user's certificate, the overall certificate managementis very expensive and complex. To address suchshortcoming, Identity-Based Public Key Cryptosystem (IBPKC) was introduced, but it suffers from the key escrowproblem as the key generation server learns the private keysof all users. Recently, Attribute Based Encryption (ABE) has been proposed that allows one to encrypt each dataitem based on the access control policy applicable to thedata. However, in addition to the key escrow problem, ABE has the revocation problem as the private keys givento existing users should be updated whenever a user isrevoked. In order to address the key escrow problem inIB-PKCintroduced a new cryptosystemcalled Certificate less Public Key Cryptography.

Disadvantages of Existing System:

- In addition to the key escrow problem, ABE has the revocation problem as the private keys given to existing users should be updated whenever a user is revoked.
- Moreover, their scheme only achieves Chosen Plaintext Attack (CPA) security. As pointed out, CPA security is often not sufficient to guarantee security in general protocol settings. For example, CPA is not sufficient for many applications such as encrypted email forwarding and secure data sharing that require security against Chosen Cipher text Attack.

Proposed System:

The proposed system of Certificate less Public Key Cryptography mainly contains three concepts i.e. Generation of group key, generation of signature, encryption and decryption of shared data in a cloud. By implementing those concepts we can improve the performance and security of shared data. The implementation procedure of those concepts as follows.

Advantages of Proposed System:

- We present the formal security model and provide the security proof. Since our mCL-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

PKE scheme does not depend on the pairing-based operation, it reduces the computational overhead.

- Unlike conventional approaches, the KGC only needs to be semi-trusted and can reside in the public cloud, because our mCL-PKE scheme does not suffer from the key escrow problem.

Generation of group key:

The key generation center will generate group key and sent to all group members. The generation of group key is as follows.

1. Each group member will register into group by entering he/she details. After registering KGC will give username and password for each user.
2. The user will login using those username and password. After login the each group member will choose two prime number(P,G) and also choose one private key a.
3. By using those values each group member will calculate public key and send to KGC. The calculation of public by using given formula.
   Public key= G^a mod p
4. The group members also sent he is prime numbers to KGC.
5. The KGC will retrieve those values and generate another public key by using give formula. Before generating public key the KGC will generate individual private keys of group members.
   Pub key_i= public $key_i^{privatekey_i}$**mod** p_i
6. After generating pub key of each member and KGC will sent to those keys to each group member.
7. Each group member will retrieve pub key and again generate shared key by using give formula.
   $sharedkey_i=pubkey_i^a$ mod P
8. After calculating shared keys each member will send those keys to Key Generation center.
9. The KGC will retrieve shared keys and will generate secret key by using following formula.

$publickey=pub_1 ® pub_2 ® .....pub_i$
$Pval=P_1 ® P_2® ……P_i$
$Secretkey_i=publickey^{sahredkey1®sharedkey2 ….sharedkey_i}$**mod**Pval

After generating secret key the key generation center will generate signature for the each group member. The generation signature is as follows.

Signature Generation:

The KGC will generate signature for authentication of each group member. The generation of signature as follows.
$Val=publickey_i®sharedkey_i$
Sig_i= hash (val)
After that the key generation center will send signature and key to individual group members.

The group members will retrieve signature and secret key again generate signature by using same formula. After generating signature both signature are equal that group member is authenticated user. By implementing this technique we can't generate any certificate for authentication purpose. So this is one of the advantages of proposed system. After completion of authentication each user will get secret key. By using the secret key each group member will decrypt the shared data in the cloud. Before sending the secret key to group member the KGC will also send the secret key to data owner for the purpose encryption of shared data and stored into cloud.

Encryption and Decryption Shared data:

In the encryption and decryption shared data can be performed by the two type of users. They are encryption process can be performed by data owner and decryption process can be performed by group member.The encryption and decryption of data by using data encryption standard. Before storing the data into cloud the data owner will encrypt the shared data and stored into cloud. After that if any user wants that

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

data it will retrieve the cipher data and decrypting by using decryption process of data encryption standard algorithm.

Conclusion:

In this paper we have propose the concept of Certificate less Public Key Cryptography. Using the Certificate less Public Key Cryptographyscheme as a keybuilding block, we proposed an improved approach tosecurely share sensitive data in public clouds. Our approachsupports three implementation processes those are the generation of secret key, generation of signature, data encryption and decryption. By implementing that concept we can't generate any certificate for the authentication purpose. We can also share the data throughout group member with securely.

Our experimental result shows more efficiency and also provides more security of shared data.

References:

[1]. Seung-Hyun Seo, Mohamed Nabeel, E Xiaoyu Ding, lisaBertino, Members of IEEE "An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds" June 2013.

[2]. Zhiguo Wan, Jun'e Liu and Robert H. Deng. Senior Member, IEEE "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" April 2012.

[3]. Mohamed Nabeel, Student Member, IEEE, Ning Shang, Elisa Bertino Fellow, IEEE "Privacy Preserving Policy Based Content Sharing in Public Clouds" 2013.

[4]. Mohamed Nabeel, Elisa Bertino Fellow, IEEE "Privacy Preserving Delegated Access Control in Public Clouds" 2013.

[5]. Yang Tang, Patrick P.C. Lee, Member, IEEE, John C.S. Lui, Fellow, IEEE, and Radia Perlman, Fellow, IEEE "Secure Overlay Cloud Storage With Access Control and Assured Deletion" November/December 2012.

[6]. SushmitaRuj, CSE, Indian Institute of Technology, Indore, India, Milos Stojmenovic, Singidunum University, Belgrade, Serbia, AmiyaNayak, SEECS, University of Ottawa, Canada, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" 2013.

[7]. SmithaSundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud" March 2012.

[8]. Junzuo Lai, Robert H. Deng, Chaowen Guan, and JianWeng "Attribute-Based Encryption with Verifiable Outsourced Decryption" 2013.

[9]. AmalAlKadi, HanoufAlYahya, CIS Department, Prince Sultan University, Riyadh, Saudi Arabia, "Data Security in Cloud Computing".

[10]. T.Divya& Mr. Arif Mohammad Abdul, A Survey on Key-Aggregate Cryptosystem for Scalable Data Sharing In Cloud Storage, IJMETMR, http://www.ijmetmr.com/olmarch2015/TDivya-ArifMohammadAbdul-39.pdf, Volume No: 2 (2015), Issue No: 3 (March)

[11]. DiaaSalama, HatemAbdual Kader, Jazan University, Kingdom of Saudi Arabia, and MohityHadhoud, Minufiya University, Egypt, "Studying the Effects of Most Common Encryption Algorithms".

[12]. AtulKahate, Tata McGraw Hill Education Private Limited, Second Edition, "Cryptography and Network Security".