A SURVRY ON SECURITY THROUGH KEY MANAGEMENT PROTOCOL IN CLOUD COMPUTING

Priya Chaturvedi[1], Umang Thakkar[2]

[1]*Student, Computer Engineering, Silver Oak College of Engineering & Technology,Gujarat, India*

[2]*Assistant Professor, Computer Engineering, Silver Oak College of Engineering & Technology, Gujarat, India*

ABSTRACT

With the growth of uses of internet and cloud computing there is ease of using and storing the vast amount of data on the net, With the immense growth of internet and its users, Cloud computing, with its incredible possibilities in ease, Quality of service and on-interest administrations, has turned into a guaranteeing figuring stage for both business and non-business computation customers.The dynamic environment of cloud results in various unexpected disadvantage. While using the internet to loading and uploading the data the main concern is protecting the data, the security is the main concern to work with cloud. It necessary to secure the private data to cloud , if not done this anybody can see and hack our private data. Cryptography that is masking the data by using key and only those download the data who have keys to decrypt or unmasking it only those person can download the data.In this survey we discuss the various key management technique of cryptography to protect our private data on cloud.

Keywords :-*Cloud computing, ABE, Security.*

1. NTRODUCTION

C*loud computing* can help to managing and monitoring task for data centers is reduced. As cloud computing give many reason or advantage to use them but it also gave a main disadvantage that is poor security. The third party is involved called CSP (cloud Service Provider) to whom provide service of cloud or the interpreter between cloud and its service. This paper surveys recent research related to security in cloud and comes up with possible solutions for preservation of security. Though cryptography is concept but key management is use to protect data, biggest security factors in cloud computing, such as data intrusion, data integrity, and service availability are handled in better way through cryptography. Research provide the best key management protocol to secure data.

1.1. Background

Cloud computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application. Three Cloud Delivery models are Iaas, PaaS and SaaS, comprises middle stratum of cloud computing environment[1]. In Software as a Service (SaaS), applications are there that are enabled for the cloud. It supports an architecture that can run multiple instances of itself which are location independent. This is nothing but a monthly subscription based pricing model and it is stateless. Examples of SaaS are MobileMe, Google docs, Zoho. Platform as a Service (PaaS) includes platform on which developers can write their applications to be run on cloud environment. This platform normally has multiple application services available for quick deployment. Examples of PaaS are Google App Engine, Microsoft AZURE, Force.com.

Infrastructure as a Service (IaaS) used by consumer by providing storage, processing, networking, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. It is highly scaled redundant and shared computing Infrastructure. Examples of this type of delivery model include Amazon EC2, Sun's cloud services. Third stratum in the cloud computing environment consists of cloud deployment models which include public, private, community, and hybrid clouds. A cloud architecture which can be accessed by multi-tenants and is available to the public is called a public cloud. Cloud which is available for a particular group is private cloud, while a community cloud is modified for a specific group of consumers. Hybrid cloud infrastructure is a combination of two or more clouds[4].

four type of deployment model that is public, private, hybrid and community cloud. Public cloud is open cloud for all, private cloud is for organization particularly and community cloud for specified community and hybrid cloud is the combination of both public and private cloud. There are so many advantages of cloud like reliability , flexibility,

scalabilty, customization, on demand ,pay per use service but as well as challenges likeSecurity and privacy, Efficient load balancing, Performance monitoring, Reliability, Availability, Portability. Our main concern is security[2].

2. CRYPTOGRAPHY

Cryptography is term of protecting the data while loading and uploading the file[2]

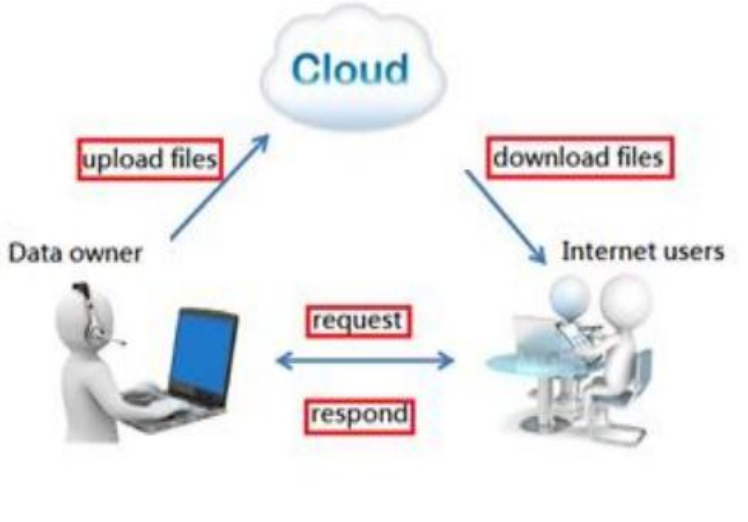

Fig 1: cryptography

In cryptography data owner upload the data in cloud and user download the file but before uploading and downloading the file must be secure by protecting ir by using the key.

As the services is provided by cloud service provider the security is necessary .the key term on security is cryptographyCryptography is the process of creating secret codes to protect the original message from attacks and maintain its integrity. Many applications use cryptography to protect sensitive data and messages. Cryptography is used to ensure that data or message remains unaltered[11] .The process of cryptography involve Plaintext which is the original message that the sender wants to send to the receiver securely.[11] Encryption is a process of converting the original message to unreadable form by using encryption algorithm with the help of a key. Ciphertext is the encrypted message produced by the encryption algorithmwith the help of a key[11].Decryption is the process of converting encrypted message to the original form using decryption algorithm with the help of a key. The key is the set of numbers on which ciphers operates.[11]

.

2.1 Type of cryptography method

2.1.1. Symmetric Algorithm

- **(DES)Data Encryption Standard**:

In this Data Encryption Standard (DES) is a symmetric- key algorithm,contains in block cipher By the side of the encryption site, DES picks out a 64-bit plaintext and inducts a 64-bit cipher text, on the decryption site, it takes a 64-bit cipher text and inducts a 64-bit plaintext, and similar 56 bit cipher key is used for both decryption and encryption. The encryption process is progress of two permutations (P-boxes), which we call preliminary and ultimate permutation, and sixteen Feistel rounds. Apiece round uses a dissimilar 48-bit round key generated of the cipher key confessing to a predefined algorithm.

- **(AES) Advanced Encryption Standard**:

Encryption with DES Standard is a symmetric- key block cipher emerged as AES equals a non-Feistel cipher. AES encrypts information with block range of 128-bits. It uses 10, 12, or fourteen rounds.Betting on the number of rounds, the key range may be 128,192, or 256 bits. AES operates on a 44 column-major order matrix of bytes, acknowledged as the state.

- **Triple-DES:**

A rather simple way of increasing, the key range of DES is to use Triple DES, to sentinel it against attacks without the necessitate to design a absolutely new block cipher algorithm. DES itself can be personalized and reused in a more sheltered scheme. Many former DES users are capable of use Triple DES (TDES) which was describe and analyzed by one of DES's patentees. It requires applying DES three times on two (2TDES) or three (3TDES) different keys .

- **Blowfish Algorithm:**

Blowfish is one of a symmetric block cipher algorithm. It us es the similar secret key to both encryp-tion and decryption of messages. The block range on behalf of Blowfish is 64 bits; messages to be a multiple of 64-bitsinside range have to be bolstered. It applies a variable length key, from 32 bits to 448 bits. It is desirable for applications where the key is not changed habitually. It is extensively faster than most encryption algorithms when did in 32-bit microprocessors with huge information caches. Information encryption detects via a 16-round Feistel network .

2.1.2 Asymmetric Algorithm

- **RSA:**

RSA cryptosystem appreciate the properties of the multiplicative Homomorphic encryption [9]. Ronald Rivest, Adi Shamir and Leonard Adleman have devised the RSA algorithm and named later on its inventors. RSA uses modular exponential for decryption and encryption. RSA uses two exponents, a and b, where a is public and b constitutes private. Let the plaintext is Pt and Ct is cipher text, thus at encryption. Ct = Pta mod n And at decryption side Pt = Ctb mod n. n is a very large number, created during key generation process[3].

- **Diffie-Hellman Key Exchange:**

(DHKE)- Whitfield-Diffie and Martin-Hellman introduced a key exchange protocol with the use of the discrete logarithm problem in the year 1976. The sender and receiver will set up and doing a secret key towards their symmetric key system, using an in sheltered channel. To set a key person A chooses a random integer a[1: n] computes ga , similarly person B computes gb for random b[1 : n] and sends it to A. The secret key is gab, which A estimates by computing (gb)a and B by computing (ga)b.

3. KEY MANAGEMENT

while again and again loading and uploading the same amount of data it become very costly and produce the challenge of key escrow problem , for this the cost of computation and ciphertext is increase and increase the problem of traffic redundancy.

For this challenge the survey suggest the different key management technique;

- **IBE AND HIBE**

It is ID based cryptography technique is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user. One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This can take place because this system assumes that, once issued, keys are always valid (as this basic system lacks a method of key revocation). The majority of derivatives of this system which have key revocation lose this advantage. Drawback of technique is If a Private Key Generator (PKG) is compromised, all messages protected over the entire lifetime of the public-private key pair used by that server are also compromised. This makes the PKG a high-value target to adversaries. To limit the exposure due to a compromised server, the master private-public key pair could be updated with a new independent key pair. However, this introduces a key-management problem where all users must have the most recent public key for the server[3].

- **RBAC**

Role-based-access-control (RBAC) is a policy neutral access control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. A study by NIST has demonstrated that RBAC addresses many needs of commercial and government organizations. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Although RBAC is different from MAC and DAC access control frameworks, it can enforce these policies without any complication. Its popularity is evident from the fact that many

products and businesses are using it directly or indirectly.disadvantage of this technique is if one employe leave the company to another than his role is shifted that produce redundancy to change the role of employee and the company also change the role

- **ABE**

ABE model was proposed by Sahai and Waters in 2005 year. ABE is the mechanism in which users are allowed to encrypt and decrypt data based on user attributes. User attributes are used to decide the secret key of the user and cipher text. If the set of attributes of the user key matches the attributes of the cipher text; then only decryption of a cipher text is possible. A crucial security aspect of attribute-based encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. There are mainly two types of attribute-based encryption schemes: Key-policy attribute-based encryption (KP-ABE)[3] and ciphertext-policy attribute-based encryption (CP-ABE)[4].
In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attributes.
Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used

- **Vo-ABE:**

verified outsourced ABE technique is work on ABE technique but also verified the sourced or the third party. For that the third party cannot access the data without the knowing of the user.
VO-ABE reduce the disadvantages of ABE like key escrow problem, key coordination and revocation technique.it work on the concept of using the extra instance to encrypt the data which verified the sourced.it decrease the computational cost of using different key for different file you can use the set of attribute to decrypt or encrypt the vast amount of file using the same set of data.[11]

4. CONCLUSION

The cryptography is necessary concept to secure the data on cloud, to protect our private data from the another user or the third party which is service provider. For this concept VO-ABE is best technique to protect data which pprotect data and verified the third party and also decrease the computational and cipher text cost.

REFERENCES

[1] Xianping Mao, Junzuo Lai, Qixiang Mei, Kefei Chen, Jian Weng Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption", IEEE, 2015

[2] Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang,"Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption",IEEE, 2015

[3] konda reddy. guddeti and gangadhara . P," An Efficient Attribute Based Encryption Data Retrieval in Cloud ",IEEE,2017.

[4] Baodong QIN, Robert H. DENG, Siqi MA," Attribute-based encryption with efficient verifiable outsourced decryption",IEEE,2015

[5] Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk," A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing",IEEE,2016.

[6] K.Priyadarsini, C.Thirumalai selvan," a survey on encryption schemes for data sharing in cloud computing",IJCSITS, 2012

[7] Guofeng Lin, Hanshu Hong, and Zhixin Sun," A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing ",IEEE, 2017

[8] Manju Khari , Manoj Kumar,V aishali , "Secure Data Transference Architecture for Cloud Computing using Cryptography Algorithms", IEEE, 2016.

[9] Omer K. Jasim Mohammad ,Safia Abbas ,El-Sayed M. El-Horbaty Abdel-Badeeh M. Salem ," Securing Cloud Computing Environment using a new Trend of Cryptography ", IEEE,2015.