A Novel Model for Key Management on Cloud
Research Article/Survey Paper/Case Study

[1]S.RAJAN, [2]Dr.D.S.MAHENDRAN, [3]Dr.S.JOHN PETER
[1]Assistant Professor and Head, Dept of Computer Science[SF], Kamaraj College, Tuticorin, Tamil Nadu, India.
E-Mail: sr_tuty@yahoo.co.in
[2]Associate Professor, Dept of Computer Science, Aditanar College, Tiruchendur, Tamil Nadu, India
E-Mail: dsmahe65@gmail.com
[3]Associate Professor & Head of Research Center, Dept of Computer Science, St.Xavier College, Palayamkottai, Tamil Nadu, India.
E-Mail: jaypeeyes@rediffmail.com

Abstract
Key management plays an important role in Cloud. Security lapse may occur in cloud due to insecure key management. In earlier days, tree based key management was used and to address the multicast key management problem, hierarchical tree method was proposed. In this way many different models such as centralized model, MPC model, hybrid system and several encryption algorithms were proposed. Each had its own advantages and disadvantages. Different key management Models and issues are analyzed and based on the issues a more secure new model is proposed in this paper.

Keywords: *key, Management, Security, Cloud, Computing.*

I. Introduction

The Evolution of Cloud doesn't occur in a single day. It took years for what we are now in the information technology of cloud. As computing complexity increased due to new technological advancement and more expectation from business organization different architectures such as single-tier, two-tier and n-tier came to exist.

[11] In Single-Tier Architecture Business logic and data logic are all present in a single machine. All the processing is done in a single machine. It is simple to design and least scalable. Mainframe Application is an example for Single-tier architecture. They are developed with batch architecture to minimize CPU power and maximize I/O Bandwidth. Due to technological revolutions in the year 80's resulted in development of PCs and minicomputers such as VAX and RISC based system. Many Organizations switched to powerful and inexpensive desktop PCs and minicomputers for their IT Solutions. This technology is known by the name Two-Tier Architecture where user interface and business logic are present in client machine and Data logic is present in server machine. Two-Tier Architecture failed for the large organizations such as Stock exchange and Banking sector so the need for new Technology arise which resulted in the Three or N-tier Architecture. As most of the computing resources are not optimally utilized, high cost resources are sitting idle most of the time. High cost involved in software development made the corporate company research for new technology that gave birth to Cloud Computing Technology which gives everything as a service. Cloud took the positive sides of fault tolerant, recovery and hypervisor technology from Mainframe Architecture. Cloud's Virtual Machine Technology was borrowed from the hypervisor Technology of mainframe computers which allowed more than one operating system in a single physical machine. It also borrowed the concepts from distributive computing, Web computing, grid computing etc. In cloud everything is given as service.

The importance of cloud is that it provides software as a service (SaS), Platform as a Service (PaS), Infrastructure as a Service (IaS). More over its distinguished characteristics is a) On Demand Self Service b) Broad Network Access c) Rapid Elasticity d) Resource Pooling e) Measured Service. These Distinguished Capabilities makes cloud computing a promising future of the upcoming Information Technology Revolution. Cloud computing along with Dev 2.0 will play a major role in IT Sector. Cloud computing is likely to witness great success from 2016 to 2023. The main drawback in cloud is security which can be achieved through effective Encryption and Decryption Techniques.

II. Encryption in cloud Computing

Securing Data in the cloud is a challenging problem as cloud environments are not trusted and are managed by either single or many third parties. It is not worthwhile to trust the third party. Organizations going for cloud should highly secure their valuable and sensitive data both present in the premise and in the cloud. To secure the data, the best possible way is to do encryption/decryption in data. The two types of Encryption algorithms are symmetric-key Encryption and Asymmetric-key Encryptions.

[3] In Symmetric-key encryption Single key is used for encryption/decryption purpose. Two different Keys are used for Asymmetric-key encryption algorithm. One key is used for encryption and another key is used for decryption. This type of encryption is used for checking data confidentiality and authentication.

Client-Side and Server-Side Encryptions are the two different types of encryption mostly used in cloud. Encrypting data on the client before sending it to server is called Client-Side Encryption. Encryption done on server while saving data is called server-side encryption. This type of encryption is used in Amazon S3. In cloud Client-Side encryption and Server-Side encryptions are mostly used.

Encryption/Decryption of data done on network end-points such as hosts or applications is called End-End Encryption. Encryption/Decryption of data at each device in a path is called Link-Level Encryption.

Encryption plays an important role to build a secure cloud. Encryption without key is not possible. Different users are assigned with different keys. The keys assigned for different users for encryption should also be encrypted with another key to make it very secure. As more and more organizations are moving their infrastructure and storage to cloud, the number of users in cloud also increases. Increase in number of users in cloud will increase the number of keys used in the cloud. So the effective key management and distribution is in urgent need for cloud. The challenges in Key Management are 1) how to share a secret key 2) when to change keys and 3) how public keys are obtained.

Possible attacks possible in key management are a) interception of any location in Network b) a key can be easily identified by the intruder if secret key is used more number of times.

III. Different aspects in Key Management

[8,9,10] Different aspects for the use of public key encryption are a) the distribution of public keys and the use of public-key encryption to distribute secret keys b) Secret key distribution with confidentiality and Authentication c) A hybrid scheme

Some techniques for the distribution of public keys are i) Public announcement ii) Publicly available directory iii) Public-key authority iv) Public - key certificates

In public announcement any participant can send or broadcast his public key to any other participants.

In publicly available directory, dynamic directory of public keys are maintained by an authority. A directory for each participant will be of the form {name, public key}. Each participant should register a public key either through person or through some secure authenticated communication. A participant may replace the existing key with a new key at any time if the private key is compromised. Periodically, the authority publishes the entire directory or updates to the directory just as hard-copy version much like a telephone book. A participant can also access the directory electronically.

Stronger security can be achieved through public-key authority. Here the central authority maintains a dynamic directory of public keys of all participants. All the participants will know the public key of the authority, with only authority knowing the corresponding private key.

In public key certificates participants can exchange keys through certificates without contacting public-key authority. Certificates are created by the certificate authority and a matching private key is given to the participants. Participants convey its key information to another by transmitting its certificate and verify that the certificate was created by the authority. Four requirements for this scheme are i) any participant can read a certificate to determine the name and public key of the certificate's owner. ii) any participant can verify that the certificate originated from the certificate authority without counterfeit iii) only the certificate authority can create and update certificate iv) any participant can verify the currency of certificate. Certificate service scheme used is X.509. The elements in X.509 schemes are Serial number, Signature, Issuer name, Period of validity, Subject name, Subjects public

key information, Issuer unique identifier, Subject's unique identifier, Extensions and Signature.

[8] Once public keys are available secure communication that thwarts eavesdropping, tampering or both are possible. Public key encryption is used mostly for distributing secret keys to be used for conventional encryption. If A communicates with B the following procedures are employed.

- $\{KU_A, KR_A\}$ Key pairs are generated by A and transmitted to B consisting of KU_A and ID_A
- Secret key K_S encrypted with A's public key is generated by B and transmitted to A
- D_{KRA} $[E_{KUA}$ $[K_S]]$ is computed to recover Secret key. A can decrypt the message only if A and B knows the identity of K_S
- KU_A and KR_A are discarded by A and KU_A discarded by B

Now A and B securely communicates by encrypting with Session key K_S

In Secret key distribution with confidentiality and Authentication A and B communicates as follows to protect against both active and passive attacks.

- A uses B's public key to encrypt a message to B containing an identifier of A (ID
  A) And a nonce (N1), which is used to uniquely identify this transaction
- B sends a message to A encrypted with KU_A and containing A's nonce (N1) as well as a new nonce generated by B (N2). Since only B could have decrypted message (1), the presence of N1 in message (2) assures A that the correspondent is B.
- A returns N2, encrypted using B's public key, to assure B that its correspondent is A
- A selects a secret key K_S and sends M-E_{KUB} $[E_{KRA}$ $[Ks]]$ to B. Encryption of this message with B's public key ensures that only B can read it, encryption with A's private key ensures that only A could have sent it.
- B computes D_{KUA} $[D_{KRB}$ $[M]]$ to recover the secret key.

In hybrid Scheme a key distribution center (KDC) is retained that shares a secret master key with each user and distributes secret session keys encrypted with master key. A public key scheme is used to distribute the master keys

IV. Issues in Key Management

[5] Some major issues in key management are a) Keys being stolen or lost b) Keys may be vulnerable to attack or compromised c) Single point of failure in key distribution center and d) linear scalability to handle lots of keys.

Issue in the distribution of public keys and public key encryption to distribute secret key is as follows. i) The disadvantage of Public announcement of public keys is that anyone can forge a public announcement. ii) In publicly available directory, an opponent by obtaining the private key of the directory authority could authoritatively pass out counterfeit public keys and subsequently impersonate any participant and eavesdrop on messages sent to any participant. Another way to achieve the same end is for the opponent to tamper with the records kept by the authority. iii) Directory of names and public keys maintained by the authority is vulnerable to tampering in public key authority scheme. If these issues are addressed properly we may provide effective key management system.

[3] The Diffie-Hellman key exchange is vulnerable to attacks whereby an intruder intercepts a message between the sender and receiver, and assumes the identity of the other party. The algorithm used in Diffie-Hellman are expensive exponential operations involved and the algorithm cannot be used to encrypt messages and can be used for encrypting secret key only

V. Related Research Work and issues in Research Area

Wang et al [12] proposed tree-based cryptographic key management for data storage in cloud. Here a single root node has the master key which can be used to derive other node keys. The party having the specific node key can access the data from that specific node. The disadvantage of this scheme is that the party having the parent key can derive the keys of the child node and access the data from that child node for which he may not have permission to do so.

Waller et al [2] worked on hierarchical tree method to address the multicast key management problem. The advantage of this schemes are a) compromised users are removed from the multicast group b) provides storage and transmission efficiency.

The common problem with tree based key management scheme is that if the outsourced party is granted a node key that node key can be used to derive all sub-keys of its child node. So only the legitimate users who can access the entire child node associated with a node should receive the node key otherwise it will result in security issue.

[1,6.7] The traditional centralized model for secure group communication over insecure channel has a key distribution center which distributes a secret key to group members, Key distribution center generates a group key, encrypts it with secret key and distributes it to the corresponding group member. This approach is easy to implement and storage efficient but it lacks to handle changes in group membership. The centralized approach also has the drawback of single point failure and hot spot attack.

In MPC, Encrypted data are computed by a set of servers. It guarantees data confidentiality even if some servers are malicious but this technology uses resources very intensively.

Sunitha rani proposed a hybrid system It has three levels. In the first level plain text is encrypted to ceaser cipher. In the second level ceaser cipher is encrypted with RSA substitution algorithm. [4] In the third level RSA is encrypted with mono alphabetic substitution. This technique took more time for encryption and decryption.

Fully homomorphic encryption is used for general computations on encrypted data and allows a user to outsource one or more cloud servers even if all servers are malicious but practically it lacks performance.

Anshu et al. [13], proposed encryption algorithm to secure cloud. In that process the author compared AES, DES, Blowfish and RSA algorithms. Comparison shows that DES consumes less encryption time. RSA takes larger memory and encryption time. Blow fish takes least memory and AES takes less time to execute cloud data.

Encrypting and Decrypting using Symmetric algorithm in cloud is faster [14]. So it is necessary to go through Different symmetric algorithms such as 1) DES 2) Double DES 3) Tripe DES and 4) Blowfish which can be used in Cloud.

DES is a block cipher [15] which operates on group of fixed bits called blocks. Plain text is converted to 64 bit blocks and encrypted with 56 bit key. The encryption/decryption process consists of initial and final permutation of transpositions with 16 rounds of substitution. The LSB of each byte is used for parity. Attacks in DES can be possible. In 1998 DES proved to be brute force attackable.

Double DES uses two keys K1 and K2. It is more secure than DES but it is prone to meet in the Middle attack.

To overcome the security flaw in Double DES, Triple DES [16] was developed. It uses three different keys such as K1, K2 and K3 for encryption and decryption. Three keying options are provided. Keying option 1 has three independent keys. Keying option 2 has two independent keys with K1=K2. Keying option 3 has identical keys with K1=K2=K3. No Known attack is found.

Blowfish [17] is a symmetric algorithm used instead of DES and IDEA. It uses variable length key from 32 bits to 448 bits. It is designed in 1993 by Bruce Schneider. It is an unpatented and license-free algorithm.

Miao Zhou in his paper [2] “Privacy enhanced data outsourcing in the cloud” proposed practical application for private data management and named it as OWUR/W (Owner Write and User Read/Write) Application where a node key in a key management tree can be shared and managed by third parties without compromising the security. [1,2] The proof of security and privacy for this approach is demonstrated through the mathematical model and no detailed practical implementation in a specific network is given. More over this scheme has more complexity if the node has multiple branches.

[18] Key management also proposed based on centralized logic tree key to adapt to the current scene.

[19] In Single Network wise key management scheme single key is stored in the node's memory, a minimum storage is occupied and there is no requirement of complex protocols to perform key discovery or key exchange since all the nodes in communication range can transfer messages using the shared key. However, there is a major security loophole in this scheme. If one of the sensor node is compromised, the communication security of the

network collapses as adversary obtains the network wide shared key. Hence it is wise for neighboring sensor nodes to establish pair wise keys just after the network deployment.

So there is a need for key management for cloud which is simple, secure, efficient, easy to implement and storage efficient.

VI. Proposed Key Management Model

To overcome the problems in tree based key management scheme and make only the legitimate user to access the data. We propose a Key management for private data Management in cloud.

Proposed Model consists of four major parties

1. **Cloud Provider** – Provides data storage services
2. **Centralized Key Distribution Center** – Trusted Third party where Data owner generates master keys. Session keys are automatically generated and encrypted with master key. Session keys are used for transmitting encrypted data to the user.
3. **The Data Owner** – Owner of the organization which hosts data on the cloud. Responsible for the key management system. Distributes Master keys manually to the user.
4. **User** – Person who access data according to their access control.

Keys used

Master Key is used for encrypting and decrypting Session Keys

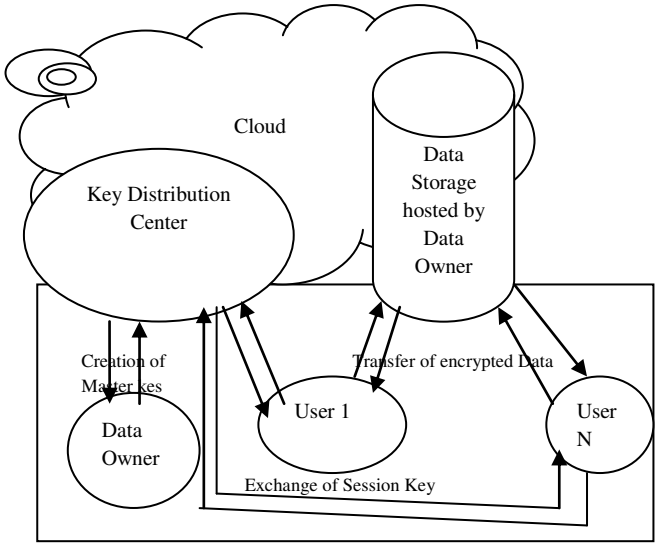
Session Key is used for encrypting data for transmission.

Symmetric key is used for encrypting and decrypting data to be stored in the cloud.

Encryption used

End-End Encryption with Centralized key Distribution. Encryption/Decryption is done on both end-points of the Network and Centralized Key Distribution is used for reducing the number of keys.

Proposed Key Management Model Diagram



VII. Conclusion

The above proposed Model titled as "A Novel Model for Key Management on Cloud" will make data accessible only to the legitimate user and it also provides three level of protection to data. The different analyses from various angles of security attack will be analyzed. More over feasibility and cost analysis will also be done.

Acknowledgement

First and foremost I thank my Research Supervisor Dr.D.S.Mahendran, Associate Professor of Computer Science, Aditanar College, Tiruchendur for accepting me as a Research Scholar and giving me an opportunity to do Research in cloud computing with valuable suggestion. I also thank my Co-guide Dr.S.John Peter, Associate Professor & Head of Research Center, ,St.Xavier College, Palayamkottai for accepting me as his Research Scholar. Last but not lease I thank Manonmaniam Sundaranar University, Tirunelveli for giving me permission to do Research in Cloud Computing.

References

[1] Weichao Wang,Zhiwei Li, Rodney Owens,and Bharat K.Bhargava.Secure and efficient access to outsourced data. InCCSW, Pages 55-66, 2009

[2] Miao Zhou, Yi Mu, Willy Susilo, Jun Yun, Liju Dong. Privacy enhanced data outsourcing in the cloud, Journal of Network and Computer Applications, 2012.

[3] William Stallings. Cryptography and Network Security, Principles and Practices, Prentice Hall 5th Edition 2014

[4] Priya Sharma. Security of Key in Cloud using Cryptography, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, issue 3, March 2015, Pages 823-826.

[5] Secure and Efficient Key Management Scheme in MANETs by Abu Taha Zamani, Syed Zubair, IOSR Journal of Computer Engineering, Issue 2, Ver. XI (Mar-Apr. 2014), PP 146-158

[6] A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET by Merin Francis, M. Sangeetha and Dr. A. Sabari, IJARCSSE Volume 3, Issue 1, January 2013

[7] Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds by Piotr K. Tysowski, M. Anwarul Hasan, IACR, 2011

[8] X. Huang, M. Yang, and S.-S. Lv, "Secure and efficient key management protocol for wireless sensor network and simulation," Journal of System Simulation, vol. 20, no. 7, pp. 1898–1903, 2008.

[9] R. Riaz, A. Naureen, A. Akram, A. H. Akbar, K. H. Kim, and H. Farooq Ahmed, "A unified security framework with three key management schemes for wireless sensor networks," Computer Communications, vol. 31, no. 18, pp. 4269–4280, 2008.

[10] An efficient group key management scheme for mobile ad hoc networks by Bing Wu, Jie Wu, yuhong Dong Int.J.SecurityandNetworks,Vol, 2008.

[11] Enterprise Cloud computing Technology, Architecture, Applications, Gautam Shroff 2010.

[12] Weicha Wang, Zhiwei Li, Rodney Owens, and Bharat K.Bhargava. Secure and efficient access to outsourced data. In CCSW, Pages 55-66, 2009.

[13] Anshu Parashar and Rachna Arora, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications, Volume 3, 2013, pp. 1922-1926

[14] Gurpreet Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, Volume 67, Issue 19, 2013, pp. 33-38.

[15] William Stallings, "Cryptography and Network Security: Principles & Practices", 4th edition, Prentice Hall, ISBN: 978-0-13-187316-2, 2005.

[16] Kaur A, Manisha Bhardwaj, "Hybrid Encryption for Cloud Database Security", International Journal of Engineering Science & Advanced Technology, Volume 2, Issue 3, 2012, pp. 737-741.

[17] Shirole Bajirao Subhash and Dr Sanjay Thakur, "Data Confidentiality in Cloud Computing with Blowfish Algorithm", International journal of Emerging Trends in Science and Technology, Volume 1, Issue 1, 2014, pp. 01-06.

[18] Yingye Cheng, Hao Li, Nan Zhang, Character-based online key management in cloud computing environment, Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2016 IEEE

19] Nazmul Islam, M.A Moyeen, An Empirical study on key Management schemes of wireless sensor Network, International Journal of Computer Applications(0975 –8887) Volume 134 – No.11, January 2016.