ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Survey on Secure Cloud Data Sharing Using Trusted Third Party

Triveni A. Bhalerao, Prof. N. P. Kulkarni

Student of Master of Engineering, Dept. of I.T., SKN College of Engineering, Pune, Maharashtra, India.

Professor, Master of Engineering, Dept. of I.T., SKN College of Engineering, Pune, Maharashtra, India.

ABSTRACT*:* Nowadays big challenge is to store data safely which can be accessible from anywhere and anytime. Data sharing and maintaining its security is practice challenge. Data owner in the data sharing system upload their files with Cryptography. If any user mistakenly leaks the key information, then it will be difficult for the Data owner to maintain security of the shared information. Unauthorized user may try few attempts and get access if partial password is known. However, it is very critical to handle key shared by the data owner. In this paper we provide a concrete and efficient instantiation of scheme to prove its security using two layers of encryption and prevention from unauthorized user by identifying them. This paper also includes survey on various papers which are based on DAC (Delegation Access Control) for Data Owner to minimize load of data owner, security of shared data through encryption which will be Two layers of encryption technique, roll based access and cost efficient certificate less encryption. TTP is one of the module to authenticate user those who have access to the data on cloud. SHA algorithm is used by TTP to generate the key, this key share to user as well as owner. TTP module get encrypted file using AES Algorithm from data owner and computes hash value using MD-5. Our system will lie between end users and cloud providers.

KEYWORDS*:* Trusted Third Party; Cloud Service Provider; Ring signature; Authentication; data sharing; privacy; cloud computing; forward security; smart grid; dual encryption; delegation access control; Cryptography.

I. INTRODUCTION

Cloud computing is emerging and trending technology in IT sector. For high pace processing and efficient access cloud plays prominent role. Today many organization switching from dedicated servers to the cloud computing. As cloud computing having servers which are dedicated and hosted. Data sharing and transferring is secure. Cloud users rely on safety given by cloud providers. This is used for users electricity usage in real time, to make email messaging services more reliable in big technology corporation, everyone can take advantage of latest technologies with spending nothing extra on infrastructure, software and IT specialists. Cloud allows data owner to store data on cloud space and user can access it from anywhere and anytime increases the availability. Along with this if cloud maintains confidentiality its a great advantage. As it is often seen cloud is intangible and transparency is less, in turns which produces insecurity about which is a correct secured and controlled cloud. In section II literature survey of based paper and detailed on schemes are explained. In section III proposed system to avoid all disadvantages to arise in literature survey, algorithms, proposed system architecture and discussion on the result and finally acknowledged for all supports. Only potential concern persist which are attack surface area, variability in terms of products and services, reliability, availability and performance guarantees. Cloud is less secure than traditional approaches, so we can make it more secure to prove is quality value when security added on it.The below mentioned diagram shows tradition approach for cloud computing [1].

II. RELATED WORK

In this section, the reference are colleced from all conferences, sites, articles, booka from the internet which helps to implement the project. For developement of this project we referred some of the base papes, ideas which hepls in development, testing and deployment phase. For good understanding of the advanced authentication system there are some work on the IEEE international journel that we have referenced are: (a) Boyang Wang, Baochun Li, Hui Li, has proposed a paper on Public Auditing for Shared Data with Efficient User Revocation in the Cloud where it gives information of Shared data with efficient user revocation in the cloud.When data owner share data among group, users in group generate signature on each block of shared data. Different blocks are signed by different user as each user working on different block of data. If unfortunately, due to security reason user is blocked, then the block signed by revoked user needs to resigned by existing user. So here existing user have to download that data and resigned which makes this inefficient. Hence, this paper provides public auditing scheme for integrity of the data and keeping user revocation efficiency in mind. (b) Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H Deng proposed a paper on Key- Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.This paper focus more on safety, flexibility and efficiency of sharing by using new public key cryptosystem by producing constant size cipher text. KAC is used for cryptography.Drawback of this scheme is that Cost is more and algorithm used are Key AggregateEncryption-Decryption. (c) Seung-Hyun Seo, Mohamed Nabeel, Member,Xiaoyu Ding, Elisa Bertinoproposed a paper on An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds. Securely share sensitive data in public clouds. Improve efficiency. This paper used medicated Certificate less public key encryption(mCL-PKE), existing mCLPKE was not efficient due to use of pairing operation which is very expensive. Here also has disadvantage that Network Connections Dependency and Cost is more algorithm used are public key encryption algorithms. This paper extends the above scheme and make partially decryption and then subsequently decrypt complete data. Again this makes it not efficient (d) Mohamed Nabeel and Elisa Bertinoproposed a paper on Privacy Preserving Delegated Access Control in Public Clouds. Decomposition ACPs used to privacy preserving fine-grained delegated access control to data in public clouds.The Owner has to handle a minimum number of attribute conditions while hiding the content from the cloud here also has disadvantage thatNetwork Connections Dependency. Cost is more algorithm used are optimization algorithms, gen graph, random cover, policy decomposition. (e) Kaitai Liang, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong proposed a paper on A DFA-Based Functional Proxy Re- Encryption Scheme for Secure Public Cloud Data Sharing. It is based on Proxy Re-Encryption (PRE) which are deterministic finite automata-based functional. Above encryption is transformed to ciphertext associated with some other string by a semitrusted proxy to whom a re-encryption key is given. That proxy cant gain access to the plaintext.Cost is more as algorithm used are DFA based functional proxy re-encryption. (f) KaipingXueand Peilin Hong proposed a pa per on A Dynamic Secure Group Sharing Framework in Public Cloud Computing. Dynamic secure group sharing framework in public cloud computing environment The sharing files are secured stored in cloud servers and all the session key are protected in the digital Envelopes. Main drawback of this scheme is if key leaked by any one user among group then it is very difficult to find out from whom key got leaked and causes security threats. Maintaining key among group and sharing makes this very complicated. (g) Tao Jiang,Xiaofeng Chen, and Jianfeng Ma proposed a paper on Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation. It has Secure data integrity auditing for share dynamic data. Provide data confidentiality forgroup users. Cost is more algorithm used are Randomized Key generation,RSA,SHA. There are various techniques which focuses on data integrity. These attempts are still away from practical use, low error detection probability, tremendous computational cost. (h) Jiawei Yuan and Shucheng Yu proposed a paper on Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification. Efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation. -Systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys. Additive Order and Privacy Preserving Function family (AOPPF) tends to allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.

.

III. PROPOSED ALGORITHM

Modification of multiuser data, public auditing, probability for high error detection, effective user revocation and computational auditing performance can be characterized by a novel integrity auditing approach for data storage and sharing services. Attack of imitation can be avoiding by given scheme. An important feature of cloud storage is data sharing. Sharing along with strong protection of data is the main aspect. Cryptography helps data owner to store data safely on cloud. While considering data privacy, we cannot rely upon traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with uploaders own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime and to anyone. First the admin saves file in the cloud space so that it will be available to users at any time. So he will generate a public key, which is used to encrypt the file. Then he chooses the file to upload and it is encrypted using public key. After encryption the file is uploaded to the cloud space. TTP generate hash code of each file which is get uploaded by the data owner. When the user needs to access the file, the admin will share the file details with the user. The generated key sent via secure Email to the user. When the user gets the Email from the admin, he will get the file details. He can now enter the file name and key to download it, in his system. After downloading the decryption is carried out with key. Then the file is saved in the predefined folder in the client system. Unauthorized access prevented by giving few preventive measures such as role based access, attack detection and preventions such as if unauthorized user trying to access data files then those are identified and user gets blocked and he/she will not be log in to the system. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analytic environment. AES is generally known for the concept which is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES works on a column 44 major order bytes matrix, termed the state. The key size used for an AES cipher specifies the number of repetitions of transformation where input which is plain text is converted into final output with applying MD rounds that is (original data + message digest), into the final output, called the cipher text (encrypted data). This needs to be repetitive and it follows the following sequence: Cycles of repetition are 10 and keys for 128 bits. Each round consists of several processing steps, each containing similar but different stages, including one that depends on the encryption key itself. Reverse process for converting cipher text to original text using the same encryption key.AES Give the input plaintext and final output is cipher text in encryption format.

1) AES
2) SHA

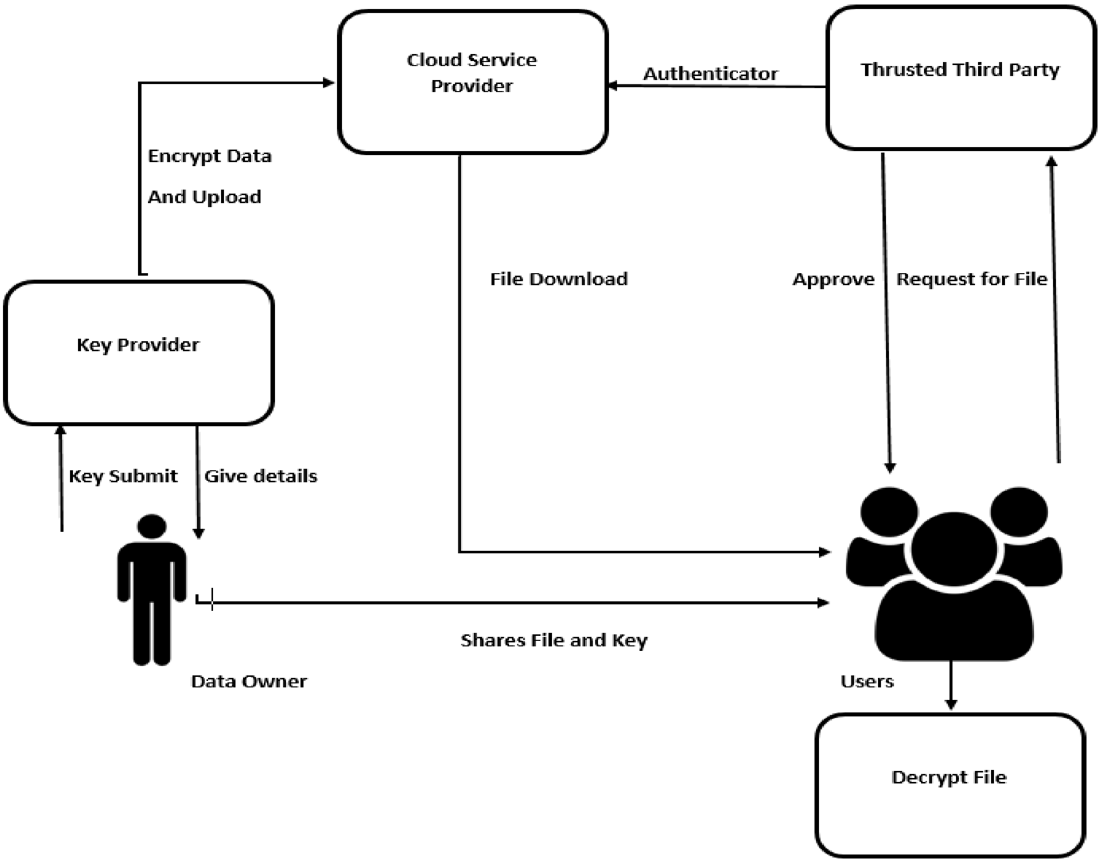

Fig:System Flow Diagram

IV. ACKNOWLEDGEMENT

For everything we achieved, the credit goes to all those who had really helped us to complete this work successfully. We are extremely thankful to P. G. Coordinator ”Prof. N.P. Kulkarni for guidance and review of this paper. I would also like to thanks the all faculty members of ”SKN College Of Engineering”.

VI. CONCLUSION AND FUTURE WORK

Motivated by the practical needs in data sharing, we proposed a new notion called authentication to only authorized user and reduce bourdon of Data owner. Secrete key size is randomly generated and key is separate for 6 each file which is uploaded on cloud server. It prevents the attack generated by unauthorized user and blocked that user permanently. In a future to enhance the security more,a mechanism to secure the key cloud can be an area of research and hardware security support on password matching scheme. To reduce the overhead of network traffic can be another area of research.

REFERENCES

[1] Rakpong Kaewpuang, Sivadon Chaisiri ” Cooperative Virtual Machine Management in Smart Grid Environment” IEEE Transactions On Services Computing,Vol.7,No.4,October-December 2014.

[2] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on ”Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.” IEEE Transactions On Parallel and Distributed System Vol.25,No.2,February 2014.

[3] Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE” proposed a paper on ”An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.

[4] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on ”Privacy Preserving Delegated Access Control in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.

[5] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong” proposed a paper on ”A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”. IEEE Transactions On Information Forensics And Security, Vol. 9, No.10,October 2014.

[6] Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on ”A Dynamic Secure Group Sharing Framework in Public Cloud Computing”. IEEE Transactions On Cloud Computing, Vol.2,No.4,October-December 2014.

[7] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on ”Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”. IEEE Transactions On Services computing Vol.8,No.1,January/February 2015.

[8] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on ”Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification”. IEEE Transactions On Information Forensics And Security,Vol.10,No.8,August 2015.

[9] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou” proposed a paper on ”Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing”. JOURNAL Of Latex Class Files, Vol. 6, No. 1, January 2015.

[10] XinyiHuang,JosephK.Liu,ShaohuaTang,Member,IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou” proposed a paper on ”Cost-Effective Authentic and Anonymous Data Sharing with Forward Security”. IEEE Transactions On Computers Vol.64.No.4,April 2015.

[11] Xinfeng Ye” proposed a paper on ” PrivacyPreservingandDelegatedAccessControlforCloud Applications”. ISSN 1007-0214 04/10 pp40-54 Volume 21, Number 1, February 2016

[12] Ovunc Kocabas, Tolga Soyata, Member, IEEE ” Emerging Security Mechanisms for Medical Cyber Physical Systems”. DOI 10.1109/TCBB.2016.2520933.