Deletion of Private Data in Cloud Computing

Vishal Pramod Rasal

M.Tech Scholar, Dept. of Computer Science & Engineering, Sandip University, Nashik.

Prof. Samadhan Sonavane
Associate Professor, Dept. of Computer Science & Engineering, Sandip University, Nashik

Abstract : **Cloud Computing has been shows their importance in the next-generation architecture of IT Enterprise. It gives centralized large data centers with collection of application software and databases, but in which services offered by the cloud providers may not be fully trustworthy. This leads about many security issues, which gives a challenging work to researcher. Till the date researcher still working to give solutions to such security challenges raised in cloud computing environment. One of the challenge is having confirmation about deleted data. In the traditional cloud environment clients storing the data in the cloud servers and paying as per the agreement did for only the time they use. After the data uploaded in the cloud servers, the client which are the data owners can see the data are properly stored or not in the cloud servers. It is also makes important that data stored in the cloud will be in encrypted format because either public cloud service providers or the other users storing data on the same server are not trusted. With the encryption of data now a days a new problems arises about the deletion of data. As user deletion will work with one-bit-return protocol: deletion program delete the data and comes with one bit answer as success or failure. This one-bit-return protocol turns the system as black box, where user needs to trust on cloud provider about deletion of data. In this paper we are presenting the data deletion process more transparent, secure and verifiable. In our proposed system we will ensure that faithful deletion of data. We also proposed the correct implementation of the data with ensured deletion of all related keys.**

IndexTerms - ***Cloud Service Provider, faithful deletion, verifiablity, encryption.***

I. INTRODUCTION:

Cloud storage could be a model of networked enterprise storage wherever knowledge is keep in virtualized pools of storage that area unit usually hosted by third parties. Cloud storage provides customers with advantages, starting from value saving and simplified convenience, to quality opportunities and climbable service. These nice options attract additional and additional customers to utilize and storage their personal knowledge to the cloud storage: in step with the analysis report, the degree of knowledge in cloud is anticipated to realize forty trillion gigabytes in 2020. Even though cloud storage system [3] has been widely adopted, it fails to accommodate some important emerging needs such as the security, abilities of auditing integrity of cloud files by cloud purchasers and police work duplicated files by cloud servers. With the event of cloud computing knowledge security becomes additional and additional vital in computing. Securely deleting knowledge from storage system has become troublesome nowadays. Common deletion operations merely mark the occupied area as free and take away entry from the directory, but some of the stored data may remain accessible for much longer. Explores the employment of cryptography and key management for firmly deleting knowledge [1]. When knowledge is keep encrypted, only the corresponding key has to be destroyed for erasing the data. Deleting data becomes a problem of managing and deleting keys. A science answer is given for deletion that creates the information deletion method. additional clear and verifiable. Here introduce assumption that sits in between specifically “trust-but verify”. Generally users assumes that once they delete a file, all the blocks that store the file are physically erased. However, traditional file deletion simply removes the metadata of the file, but leaves the file data intact [1]. This may violate user privacy, because the deleted file can be easily recovered. Another general misconception is that if a file was overwritten, the previous version of the file cannot be restored. In case of magnetic media such as a hard disk, the file can still be recovered, even if the file data was overwritten. There are two types of secure deletion schemes, overwriting and encryption [2]. TPM communicates with host, following a secure storage and erasure (SSE) protocol. This is the central component within the entire system style.

II. LITERATURE SURVEY

In this section, we have a tendency to square measure presenting the analysis work of some outstanding authors within the same arena and explaining a brief report of varied strategies used for secure information in cloud computing. Akli Fundo, Aitenka Hysi Igli Tafa analysed same techniques of erasing data from the disk from hard drives can also be used on SSD’s. For erasing a file from disc drive from SSD’s cannot use a same technique, so as to form this potential, some charges are required in file layer, file layer is used for mapping between physical address and logical address .Here author tried to analyse different methods to erase data from SSD’s and to see which method gives the best result .Four levels of clearing knowledge from storage media: initial level is Logical Clearing: By over writing uses will delete Indian file or enter disk logically. Second level is Digital Clearing: Here, it is impossible to recover the data in a digital way. Third level is Analog Clearing: Signal that encodes the info is broken during this level it's not possible to construct the signal. Alternative way to hide the bits Cryptographic Clearing: This level uses a key, in order to encrypt and decrypt the data which enter and exit .From physical media someone can extract the key avoid the encoding. By examination these strategies author completed that initial methodology, had a 0.5 success, second methodology is additional undefeated than initial methodology. It has some fails in it, third method, is of no use because it does not guarantee the deletion [2].

For secure deletion Z.N.J. Peterson, R.Burns, J.Herring, A.Stubblefield, A.D.Rubin compares two methods that uses a combination of authenticated encryption: Encrypting a file with key and securely disposing of the key to make the data unrecoverable .The files that write knowledge on disk ,data maybe securely deleted by the corresponding encrypt without a key, data may never be decrypted and read again and secure overwriting: Original data cannot be recovered .secure overwriting has performance concern in versioning systems For the research and commercial applications versioning storage system are important .Secure deletion is the act of remaining digital information from a storage so that it can never be recovered . Here say that, a data is encrypted and converted into a cipher text block and a small slab. Securely overwriting the block makes the corresponding block is recoverable. Here they present a two algorithms. First algorithmic program employs the all-or nothing rework so firmly overwriting a block or any 128 bit block of a cipher text firmly deletes the corresponding disk block .second algorithm generates a random key per block in order to make encryption no repeatable [4].

J.Reardon, D.Basin, S.Capkun present a taxonomy of adversaries differing in their capabilities as well as a systematization for the characteristics of secure deletion approaches. Characteristics includes environmental assumptions, such as the deletion latency and physical ware. Here during this paper say well by organizing the approaches in terms of interfaces to the physical medium. Here they organize secure deletion approaches into the layers through that key address the physical medium. Once secure deletion is enforced at one layer, then the higher layer, interfaces can explicitly offers this functionality. There are two common use level approaches. First, Environmental Assumption: embrace the expected behaviours of the system underlying the interface. Second, behavioral Assumption: includes the deletion latency and also the wane the physical medium. S.Garfinkel, A.Shelat, during this paper, say that there ar many ways to assure privacy data. One of the oldest and most common techniques is Physical Isolation: keeping confidential data on computers that only authorized individual can access [6].

Cryptography is associate degree another tool that may assure data privacy. User will cipher information because it is shipped and decipher it at the meant destination mistreatment for eg: Secure Socket Layer (SSL) encryption protocol. In absent of crypto graphical filing system, direction is quickly accessible once homeowners improperly retire these disk drives. D.Boneh, R.Lipton presents an system which enables user to remove a file from both the file system and all backup topics on which the file is stored. New way of cryptography is applied, cryptography is used to erase information rather than protect it the backed up files are stored for extending periods of time it is desirable that the block cipher wont to inscribe the files be extraordinarily secure. Also say about standard UNIX backup utilities, user enable to specify a collection of files that should not be backed up [7].

M.Abdalla, M. Bellare and P. Rogaway provides security analysis for the public key encryption scheme DHIES and is now in several draft standards [8]. DHIES is a Diffie Hellman based scheme that combine a symmetric encryption method authentication code and a hash function, in addition to number theoretical operations, in a way which is intended to provided security against chosen cipher text attacks. It also introduce about natural assumptions under which DHIES achieves security under chosen cipher text attack .those assumptions are hash DH assumption (HDH), oracle DH assumption (ODH) and the strong DH (SDH). Sarah Diesburg, Christopher Meyers, Mark Stanovich, Michael Mitchell, Justin Marshall, Julia Gould, and An-I Andy Wang introduces True erase, a holistic secure deletion framework. True erase shows that it is possible to build a legacy-compatible full storage data path framework that performs profile secure deletion and works with common file systems and solid state storage while handling common system failures. In addition, framework will secure as a building block for coding and tainting based mostly secure deletion system. Here say that may opportunities exists to increase true erase performance on NAND flash [9].

Mohammed Achemlal, Said Gharout and Chrystel Gaber explains about the possibility of using TCG (Trusted Computing Group) specifications to establish trust in cloud computing especially between the provider of cloud computing infrastructure and his customers and also describes the context and the motivations that lead to TCG specification and also describes the functions and properties of TPM (Trusted Platform Module) which is the root of trust in TCG and also say that several approaches to adopt TPM in order to build trust in cloud computing [10].

III. PROPOSED FRAMEWORK

In this paper, we present a Trusted Platform Module (TPM) which ensures the faithful deletion of the data with keys used for encryption. Usually the traditional approach was a black box system were user only get one-bit-return value about success or failure of deletion. But as cloud providers or the users accessing the same public cloud were untrusted, so first measure to deal with is storing the encrypted data in the cloud. But the keys used for encryption and decryption of those stored data must be deleted after the use. User is totally unaware about the physical deletion of such keys in cloud. So to build the transparent system we proposes here the system which not only transparent but also secure and verifiable too.

The proposed system will be divided into several independent modules:-

1. Public cloud owner
2. User request
3. Make secrete data
4. Key distributer

1.Public cloud owner: In this module main work are based on admin approval system. If admin can approve to deleting the data from admin side to cloud server this server can take some extra backup about public verifiable data with the verification on secrete key method.

2. User request: In this module are have request role to admin side and it can do this work based on user public data.

3. Make secrete data: In this module are used to make some data from user side to request side it may occur some useful data, secret data and useless data they always manipulated from public cloud.

4. Key distributer: In this project main role are key distributer they can used to delete some secrete data from public cloud from cloud server with the help of authorized mobile number? They need some basic information about current user.

The figure below depicts our proposed system.

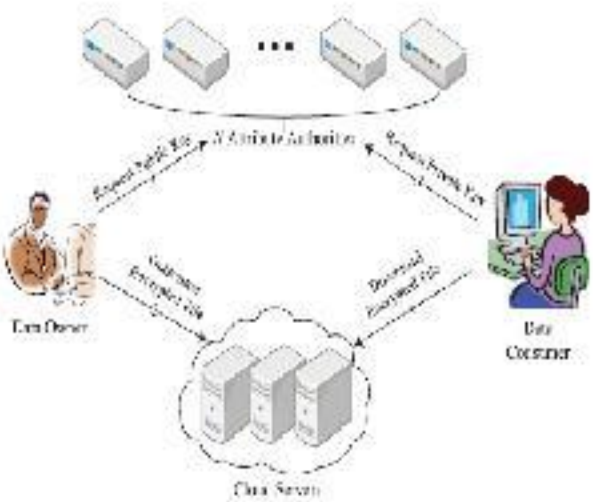

Figure 1. Architecture of Proposed System

SSE Protocol:
With Secure Storage and Erasure (SSE) protocol TPM communication happens. Following API functions are an overview, the SSE protocol specifies:

- **KeyGen**. To generate a random public/private key pair;
- **Encrypt**. To encrypt data with a specified public key;
- **Decrypt**. To decrypt data with a specified private key;
- **Audit**. To audit if encryption was done correctly;
- **Delete**. To delete a particular private key returned as a proof of deletion.

While accessing all above functions, the user needs be be authenticated himself first. This can be archived in different way: like, passwords, biometrics, etc. To make it simple, we assume that user will pass the authentication phase and able to call the functions.

VI. CONCLUSION

In this paper, we have proposed a system which gives verifiability about the deletion of data. It is not only verifying about the normal data deletion but also verifying deletion of all keys used for encryption and decryption purpose. Our main purpose is to make data deletion process transparent, secure and verifiable. We also are going to use the encryption for storing the data in the cloud so to give secure environment to users. This data deletion is done with the user's permission so that privacy and security both can be maintain simultaneously.

V. REFERENCE

[1] Feng Hao,Member, IEEE, Dylan Clarke, and Avelino Francisco Zorzo, "Deleting Secret Data with Public Verifiability", IEEE Transaction on Dependable and Secure computing, VOL. 13, NO. 6, NOVEMBER/DECEMBER 2016.

[2] Akli Fundo, Aitenka Hysi,Igli Tafa, Polytechnic University of Tirana, "Secure Deletion of Data from SSD" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No.8, 2014.

[3] Juels.A and J. Burton, S. Kaliski, "Pors: Proofs Of Retrievability For Large Files",In Proc. ACM Conf. Computer and Comm. Security (CCS‟07), pp. 584-597, Oct. 2007.

[4] Z.N.J. Peterson, R. Burns, J. Herring, A. Stubblefield, A.D.Rubin, "Secure Deletion for a Versioning File System, "Proceedings of the 4th Conference on USENIX Conference on File and Storage Technologies (FAST), Vol. 4, pp. 143-154, 2005.

[5] J. Reardon, D. Basin, S. Capkun, "SoK: Secure Data Deletion," Proceedings of the 2013 IEEE Symposium on Security and Privacy, pp. 301-315, 2013.

[6] S. Garfinkel, A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, Vol. 1, No. 1, pp. 17-27, 2003.

[7] D. Boneh, R. Lipton, "A Revocable Backup System," Proceedings 6th USENIX Security Conference, pp. 91-96, 1996. M. Abdalla, M. Bellare and P. Rogaway, "The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES," Topics in Cryptology - CT-RSA'01, LNCS Vol. 2020, 2001.

[8] M. Abdalla, M. Bellare and P. Rogaway, "The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES," Topics in Cryptology - CT-RSA'01, LNCS Vol. 2020, 2001

[9] S. Diesburg, C. Meyers, M. Stanovich, A. Wang and G. Kuenning, " TrueErase: Per-File Secure Deletion for the Storage Data Path ", ACM Transactions on Storage, vol. 12, no. 4, pp. 1-37, 2016.

[10] M Achemlal, S.Gharout,C.Gaber, "Trusted Platform Module as an Enabler for Security in Cloud Computing",Proc.Conf. on network and information system security(SAR-SSI), 2011