Analysis of Data Security in Cloud Computing: A Review

Juhi Yadava[1], Prof. S. R. Yadav[2]

[1]*PG Scholar,* [2]*Head, Department of CSE*

MIT, Bhopal, India

Abstract: Cloud computing is envisioned as the next-generation technology. It is an Internet based technology where quality services are provided to users including data and software, on remote servers. Advantages of cloud computing includes creating and storing data at remote servers, hence utilizing the client resource to the minimum level. But this advantage implicitly contains drawback of data security and privacy vulnerabilities. There are a number of algorithms and methodologies available for achieving data security in cloud computing. In this paper we look at the current researches related to data security issues like integrity and confidentiality. In particular, we will discuss how to secure client's data on remote cloud servers.

Keywords: Trusted Storage, confidentiality, integrity, Kerberos services, reliability.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams [1]. Cloud storage is simply a term that refers to online space that you can use to store your data. As well as keeping a backup of your files on physical storage devices such as: external hard drives, sub flash drives, etc [2]. Example of cloud computing: Amazon Cloud Drive, G Space, Minus, Web e-mail providers like Gmail, Hotmail and Yahoo! Mail store e-mail messages on their own servers, A Drive YouTube, Social networking sites like Face book and MySpaceSites like Flicker and Picasa host millions of digital photograph. As with any storage system, there are certain security properties that are desirable in a cloud storage system: confidentiality, integrity, write-serializability and read freshness. These properties ensure that user's data is always secure and cannot be modified by unauthorized users and the data is always at the latest versions when being retrieved by the user. [3] Storing important data with cloud storage providers comes with serious security risks. The cloud can leak confidential data, modify the data, or return inconsistent data to different users. This may happen due to bugs, crashes, operator errors, or mis-configurations. Furthermore, malicious security breaches can be much harder to detect or more damaging than accidental ones: external adversaries may penetrate the cloud storage provider, or employees of the service provider may commit an insider attack. [4] These concerns have prevented security conscious enterprises and consumers from using the cloud despite its benefits [5].

II. DISCUSSIONS

A. Problem Statement

Security and reliability are main challenges of cloud computing. Clients aren't likely to entrust their data that on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available[1]. Some of these techniques are:

Encryption**:** technique use complex algorithm to hide the original information with the help of encryption key. Authentication processes, which require creating a user name and password.

Authorization practices –firstly list of authorized clients, who can access data stored on cloud system. However, many people worry that data saved on a remote storage system is vulnerable. . Hackers could also attempt to steal the physical machines on which data are stored. A disgruntled employee could alter or destroy data using his or her authenticated user name and password. Cloud storage companies invest a lot of money in security measures in order to limit the possibility of data theft or corruption. We are discussing some techniques that are helping how to get security at administrative level and for different clients by doing survey and reading the different research paper. In this article we look at the Trusted Platform Module (TPM) to get confidentiality and integrity in clouds. Kerberos services to authenticate the users and SLA Proof for retrieving write serializability, and freshness in clouds.

III. A TRUSTED STORAGE SYSTEM FOR THE CLOUD

The main task of is **"A Trusted Storage System"** not only storing the data as well as it needs confidential storing also and integrity of the data would be maintained. To achieve confidentiality and integrity of the data, cryptographic techniques can be used to encrypt data. Encrypted file systems (EFS) can be used to encrypt the client's data within the cloud. An encrypted file system is used to encrypt the user's data, manage and create keys which are used for data encryption and decryption "[6]. Integrity of the data within the cloud is developed. Five protocols are developed which ensure that the client's data is stored only

on trusted storage servers, replicated only on trusted storage servers, and guarantee that the data owners and other privileged users of that data access the data securely. The system is based on trusted computing platform technology [7].

A. Encrypted File Systems

EFS (Encrypted File System) meant for encrypting stored files. Encryption procedures are transparent to the user and occurs at the file system level not at the application level. These methods automatically use cryptographic techniques for encryption; hence user saves from cumbersome task of managing keys in encryption. Diagram below depicts the process of encryption using EFS:

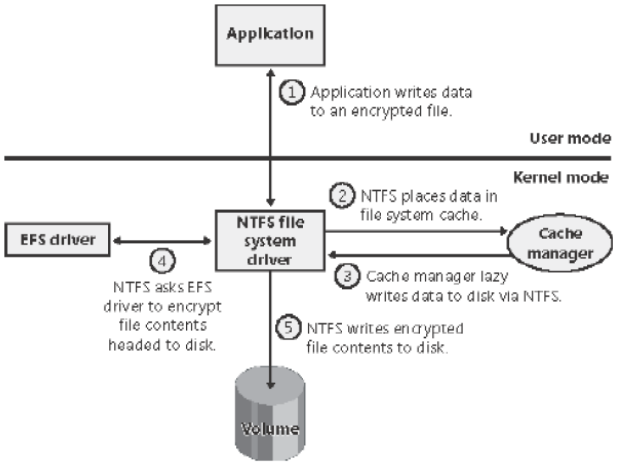

Figure 1: Example of flow of an encryption process in an Encrypting File system

Process explanatory steps are as follows:

Data passes from application part to the NTFS file system driver.

NTFS passes data to Cache Manager, whose responsibility is to write data to the disk using NTFS. NTFS passes the data to EFS driver for encryption. EFS driver encrypts data and responds to NTFS with data and encryption/decryption keys. NTFS finally writes data and associated keys on the disk.

B. Trusted Platform Module

What is a TPM?

The Trusted Platform Module (TPM) is a computer microchip or a microcontroller which is designed to perform various security-related and cryptographic functions. It can securely store the artifacts used to authenticate the platform of a computer.[9] The artifacts can include encryption keys, certificates, passwords, and integrity metrics of a platform. The TPM can be used in the process of remote attestation of a platform of a machine which will be discussed further later. It is typically installed on the motherboard of a computer. The TPM uses a hardware bus to communicate with the rest of the system. The TPM is a specification or implementation of that specification as a chip. The specification is provided by the Trusted Computing Group [10].

C. Architecture of the TPM

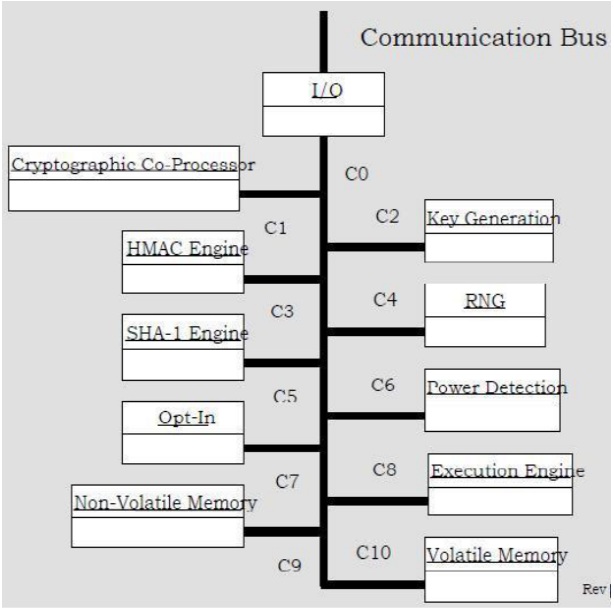

Figure 2: Component Architecture of a TPM

Short description of the different architectural components is as follows:

The input and output component is for controlling information flow through communication bus. It does controlling by sending/receiving messages to appropriate components. Cryptographic Co-Processor component performs cryptographic functions like Asymmetric Key Generation (RSA), Asymmetric Encryption/Decryption (RSA), Hashing (SHA-1), and Random Number Generation (RNG), with in TPM. RSA key pairs and symmetric keys are generated by Key Generation Component. HMAC engine solves two main purposes. First purpose is proof of knowledge of user data authentication and second purpose is authentication of request received by TPM. RNG generates random values. These random value acts as nonce for key generation, also plays role in having randomness in signatures. SHA-1 Engine functions during machine boot time, for platform measurement. Power detection component manages the power states in TPM, synchronized with platform power states. Opt-In component functions for following states of TPM:

Turn-on and Turn-off, Enable and Disable, Activate and Deactivate

Execution Engine responsible for execution the TPM commands received from the I/O component. Non-Volatile Memory component is for storing identity and state of TPM persistently. Entities authorized by TPM owner can also use Non-Volatile Memory for data storing.

Result of Trusted Storage system:

By using TPM model, security can achieve only for system administrative level. But there is no solution for individual users because cloud is maintained by third party on network. This proposed system gives confidentiality and integrity of the data stored only on trusted storage server.

IV. ENSURING DATA STORAGE SECURITY IN CLOUD COMPUTING WITH EFFECT OF KERBEROS

In this technology we ensure cloud storage security with the help of Kerberos authentication service. That is by implementing the Kerberos; security would be achieved for users. We define the Kerberos for create the ticket and granting ticket for each user. So to make the more focus on user we made more secure [12].

Kerberos operation

Kerberos use strong encryption method and complex ticket granting algorithm [12] so that user can be authenticated on network. It also uses session key which allow encrypted data stream over an IP network for each user. If new user wants to use the cloud then he should make profile on network by providing information then attributes like user ID, hashed password will save in the large Data Base. All user are registered with the Kerberos server have user ID and passwords.

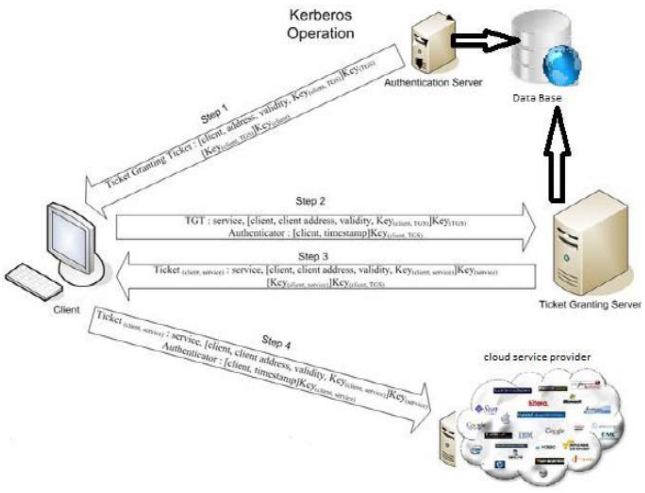

Figure 3: Cloud data storage architecture

Following steps must be taken by each user for using cloud data:

Log on to workstation.

Send the request for ticket granting ticket to the AS. AS verifies user's access right in database, create ticket-granting ticket and session key. Results are encrypted using key derived from user password. User will send the request cloud service granting ticket to TGS. TGS will send the Ticket + session key to the user (it execute one per type of service). Workstation sends ticket and authenticator to cloud server provider. Server verifies ticket and authenticator match, then grant access to service. Here assumption is that each user, who connects and utilizes the cloud server, must create the profile and provide some private information for more security of his data at cloud servers.

V. ENABLING SECURITY IN CLOUD STORAGE SLAS WITH CLOUD PROOF

I did another survey on cloud storage security based on "Enabling Security in Cloud Storage SLAs with Cloud Proof". According to this survey it presents a Cloud proof, a secure storage system specifically designed for cloud. In cloud proof customers can not only detect violations of integrity, write-serializability, and freshness, they can also prove the occurrence of these violations to a third party [13].

System Overview of cloud proof:

Cloud Proof has the following four goals.

Goal 1: Users should detect the cloud's violations of integrity, freshness, and write-serializability. Users should provide confidentiality to themselves by encrypting the data they store on the cloud.

Goal 2: Users should be able to prove cloud violations whenever they happen. Any proof system has two requirements:

(1) The user can convince a third party of any true cloud violation; and

(2) The user cannot convince a third party when his accusation of violation is false

Goal 3: Cloud Proof should provide read and write access control in a scalable (available) way. Since we are targeting enterprise sizes, there may be hundreds of thousands of users, many groups, and terabytes of data. We want to remove data owners from the data access path as much as possible for performance reasons. Owners should be able to rely (in a verifiable way) on the cloud for key distribution and access control, which is a highly challenging task.

Goal 4: Cloud Proof should maintain the performance, scalability, and availability of cloud services despite adding security. The overhead should be acceptable compared to the cloud service without security, and concurrency should be maintained. The system should scale to large amounts of data, many users per group, and many groups, since this is demanded by large enterprise data owners.

VI. CONCLUSIONS

In this discussion we found various solutions to enforce the security for data stored on cloud. In this paper we demonstrate how confidentiality and integrity security can be achieved by using DaSCE techniques. Kerberos proofs

the authentication of users on network. SLAs with Cloud Proof build confidentiality, integrity, write-serializability and read freshness (denoted by C, I, W, F). Providing privacy to customer and his data on cloud is very complex and cost effective system.

REFERENCES

[1] Mazhar Ali, Saif U. R. Malik, Samee U. Khan, **"**DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party**",** IEEE Tran on Cloud Computing, 2017.

[2] M. S. Blumenthal, "Is Security Lost in the Clouds?"Communica-tions and Strategies, No. 81, 2011, pp. 69-86.

[3] C.Cachinand M.Schunter, "A cloud you can trust,"IEEESpectrum,Vol. 48, No. 12,2011,pp. 28-51.

[4] C. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols." In Computer Aided Verification, Springer Berlin Heidelberg, 2008, pp. 414-418.

[5] Cloud Security Alliance https://downloads.cloudsecurityalliance.org/initiatives/cdg/CSA_CCAQIS_Survey.pdf (accessed March 24, 2013).

[6] W. Diffie, P. C. V. Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges,"Designs, Codes and Cryptography,Vol. 2, No. 2, 1992, pp. 107-125.

[7] M. Ali, K. Bilal, S. U. Khan, B. Veeravalli, K. Li, and A. Y. Zomaya, "DROPS: Division and Replication of Data in the Cloud for Opti-mal Performance and Security," IEEE Transactions on Cloud Com-puting, 2015, DOI: 10.1109/TCC.2015.2400460.

[8] N. En and N. Srensson, "An extensible SAT-solver," Lecture Notes in Computer Science, vol. 2919, Springer, 2003, pp. 502-518.

[9] C P. Gomes, H. Kautz, A. Sabharwal, and B. Selman, "Satisfia-bility solvers," In Handbook of Knowledge Representation, Elsevier, 2007.

[10] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud compu-ting: Opportunities and challenges,"Information Sciences,Vol. 305, 2015, pp. 357-383.

[11] A. Juels and A. Opera, "New approaches to security and availabil-ity for cloud data," Communications of the ACM,Vol. 56, No. 2, 2013, pp. 64-73.

[12] S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security,Springer Berlin Heidelberg, 2010, pp. 136-149.

[13] M. Kaufman,"Data security in the world of cloud comput-ing,"IEEE Security andPrivacy,Vol. 7, No. 4, 2009, pp. 61-64.

[14] H. Lin and W. Tzeng, "A secure decentralized erasure code for distributed network storage," IEEE Transactions on Parallel and Dis-tributed Systems, vol. 21, no. 11, Nov. 2010, pp. 1586-1594.

[15] H. Lin and W. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, June 2012, pp. 995-1003.

[16] S. U. R. Malik, S. K. Srinivasan, S. U. Khan, and L. Wang, "A Methodology for OSPF Routing Protocol Verification," 12th Inter-national Conference on Scalable Computing and Communications (ScalCom), Changzhou, China, Dec. 2012.

[17] L. Moura and N. Bjrner, "Satisfiability Modulo Theories: An appetizer," Lecture Notes in Computer Science, Vol. 5902, Springer, 2009, pp. 23-36.

[18] T. Murata, "Petri Nets: Properties, Analysis and Applications," Proc. IEEE, Vol. 77, No. 4, pp. 541-580, Apr. 1989.

[19] A. Shamir, "How to Share a Secret," Comm. ACM, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

[20] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and privacy challenges in cloud computing environments,"IEEE Security andPrivacy, Vol. 8, No. 6, 2010,pp. 24-31.

[21] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.

[22] A. Yun, C. Shi, and Y. Kim, "On protecting integrity and confiden-tiality of cryptographic file system for outscored storage," Proceed-ings of 2009 ACM workshop on cloud computing security CCSA'09, pp. 67-76, 2009.

[23] M. Ali, R. Dhamotharan, E. Khan, S. U. Khan, A. V. Vasilakos, K. Li, and A. Y. Zomaya, "SeDaSC: Secure Data Sharing in Clouds," IEEE Systems Journal,2015,http:// dx.doi.org/10.1109/JSYST.2014.2379646.

[24] A. R.Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models,"IEEE Communica-tions Surveys and Tutorials,2013,1-21.