Survey Paper on Encryption, Authentication and Auditing Services for better Cloud Security

Aishwarya Gupta
Krishna Engineering College
Ghaziabad, Uttar Pradesh

Vishwajeet Pattanaik
Krishna Engineering College
Ghaziabad, Uttar Pradesh

ABSTRACT

Data Storage Security is matter of concern especially in the field of Cloud Computing where large amount of data is being stored on daily basis over the internet. But the real world is facing some or other challenging issues regarding the same. An ubiquitous and an on-demand access with an interoperable network of your various computing resources and sharing necessary information is the need of this Internet dependent Earth, which has led the generation of Cloud and the virtual world related to it. As the number of users and data over the net are getting increased second by second there is a need of system or method which could hold this with all its privacy, integrity and confidentiality. But the vulnerabilities over Cloud data are weakening the expected progress of the field. Many complex encryption and decryption techniques are being introduced but the new risks get generated. The organisation at every level is concerned with privacy of the data and various attacks which don't enable them to use the Cloud's benefits and its susceptibility over the data holds the technology to grow. Some trustworthy and dependable Cloud storage will be a good option with the specific authentication as well as proper agreements and auditing protocols defines earlier itself will motivate the people to be secure and tension free while storing the data over the Cloud.

General Terms

Cloud Computing, Data storage security.

Keywords

Cloud Computing, Data Storage Security, Encryption as well as Decryption Algorithms, Trusted Storage Platform, Kerberos, Third Party Auditor.

1. INTRODUCTION

The Cloud Computing technology has been in focus and in demand for the last few years. Cloud computing directly refers to the process of storing and accessing data and programs over the internet. It reduces the overhead of the data storage in laptops and hard disks, maintenance cost, and provides the useful and the effective underlined information with all the pros and cons within nanosecond on our demand with an accurate and precise computation if required. Cloud promises huge cost benefits, agility and scalability to the business. It is perfectly elastic and flexible for whatever data you want to save or retrieve. Cloud computing has given a new dimension to the complete outsourcing arena. There are major 3 service models which forms the baseline for the Cloud are as:

Software as a Service (SaaS): In this type of model the software are being provided by the organisation to the clients through the web browser so that company don't need to carry heavy databases on the systems. It is also called as "on-demand software service".

Platform as a Service (PaaS): Cloud providers provide various platforms for deployment of client's application, over the internet or say Cloud but don't allow them to access it on their own. They just provide the platform to be used as a service.

Infrastructure as a Service (IaaS): In this model of Cloud Infrastructure is being provided to the client for storage, accessing, transactions, processing other important resources from one place to other. The client can deploy and execute is application using these infrastructure. The basic feature it provides to users is that it frees them from all the overhead expenses of infrastructure, networks and storage too. The clients are charged on per-use basis according to the usage.

An important advantage that Cloud serves over the computer is to store data in the available space and retrieve information whenever and wherever requested by the authenticated user. Major Cloud providers are Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2), Microsoft's Azure, Google's App Engine, and many more. [1].

On one hand we are in great need of outsourcing our big data to the Cloud for grasping its benefits and advantages properly and completely up to mark. On the other hand, security remains the critical issue that concerns potential clients, especially for the banks and government sectors [1]. A major challenge for any comprehensive access control solution for outsourced data is the ability to handle requests for re-sources according to the specific security policies to achieve congeniality, and at the same time protect the users' privacy.

Each of these issues can be addressed at various levels and subsystems of Cloud computing computer systems on the client and server sides, and in the network joining these systems. The level of these functions range from low-level hardware implementations to virtual machines and hypervisors, finally leading to operating systems and then all the way to user visible application.

Data integrity can be described as the accuracy and consistency of stored data. It actually keeps a check on the data which has been transferred over the net that it had not been modified or intruded by any other unauthenticated user through any malicious activity. It also includes "origin" or "source integrity" that the data actually came from the person or entity you think it should be, rather than an imposter. Integrity is nothing but the information which reflects the actual circumstances and also validates the data under the same circumstances which would generate similar reliable data.

Data confidentiality is the concept of trusting the source from where the data is being transacted for processing. Further there will be a discussion of some techniques which maintain the integrity and confidentiality of the Cloud data by using good encryption decryption techniques like AES, RSA, SHA-1, MD-5, etc. as well as authentication protocol with the help of KERBEROS and some applications to keep a check on the data security by adding some SLA'S AND TPA'S. But for better integrity and security purpose there should be inculcation of approaches and techniques that serves and allows the Cloud to be risk free and somewhat more efficient to be use by the users.

2. ENCRYPTION AND DECRYPTION SERVICES

Both of these aspects can be fulfilled by having a good and an effective encryption and decryption techniques. Various techniques used in present are:

- Rivest, Shamir, and Adleman (RSA).
- Advanced Encryption Algorithm (AES).
- Secure Hash Algorithm (SHA).
- Message Digest-5(MD-5)

2.1.Rivest Shamir Adelman Algorithm (RSA)

RSA is an asymmetric key cryptography uses key exchange method. RSA contains 2 keys: Public-Key and Private-Key. In Cloud environment, Pubic-Key is known to everyone, whereas Private-Key is known only to the user who originally owns the data. The data is encrypted by the Cloud service provider and the Cloud user can decrypt it accordingly with the help of the keys. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps (see Figure 1):

2.1.1. Key Generation:

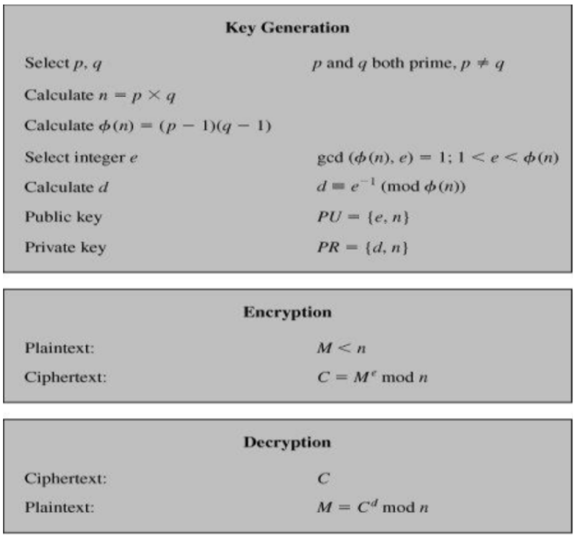
- Choose two distinct prime numbers a and b. The integers a and b should be chosen at random and should be of similar bit length.
- Calculate n = a * b.
- Calculate the value of Euler's Totient function,
  Ø (n) = (a-1) * (b-1).
- Chose an integer e, such that 1 < e < Ø (n).
- GCD (Greatest Common Divisor) of e and Ø (n) is 1. Now e will behave as a Public-Key exponent.
- Now we calculate d as follows: d = e-1(mod Ø (n)) i.e., d is multiplicative inverse of e mod Ø (n).
- d is kept as Private-Key component, so that
  d * e = 1 mod Ø (n).
- The Public-Key contains modulus n and key exponent e i.e., (e, n).
- The Private-Key consists of d and e (d, e), which is kept secret from all [6]

2.1.2. Encryption:

- Cloud service provider transmits the Public- Key (n, e) to the users who want to keep the data with him.
- User data is mapped to an integer by using a reversible protocol called as padding scheme which helps in managing the extra bits efficiently.
- Data is encrypted and the resultant cipher text (data) C is C = M^e(mod n).
- Thus the data got encrypted [6].

2.1.3. Decryption:

- The Cloud user requests the Cloud service provider for the data.
- Cloud service provider verifies the user's authentication and gives the encrypted data i.e., C.
- The Cloud user can decrypt the data by calculating, m = C^d(mod n).
- Once m is obtained, the user can get back the original data by reversing the padding scheme [6].



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Fig 1: Steps followed in RSA

2.2. Advanced Encryption Algorithm (AES)

AES which was introduced after when various drawbacks of DES (Data Encryption Standard) by Rijindael available in 3 sizes of key: 128, 192 and 256 bits. It has non feistel structure. For encryption, each round as shown in (see Figure 2) consists of the following four steps:

2.2.1. Sub Bytes

A non-linear substitution step where each byte is replaced with another according to a lookup table (S-box) [15].

2.2.2. Shift Rows

A transposition step where each row of the state is shifted one after other in a cycle certain number of times [15].

2.2.3. Mix Columns

A mixing operation which operates on the columns of the state, combining the four bytes in each column [15].

2.2.4. Add Round Key

Each byte is combined with the round key and each round key is taken from the cipher key by using schedule [15].

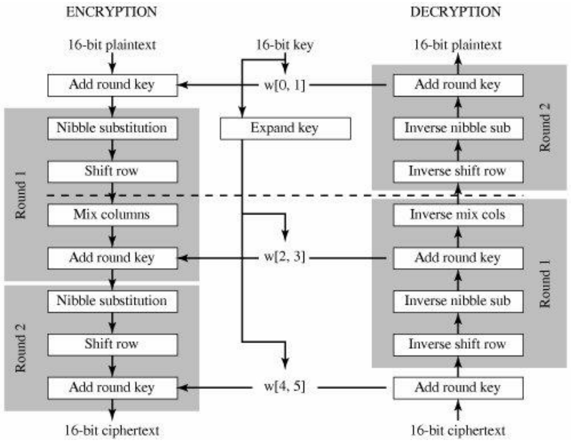


Fig 2: Processing of AES Algorithm

3. TRUSTED STORAGE PLATFORM SERVICES

We also have Trusted Storage Platforms for the Cloud's confidentiality and integrity of the data. The Trusted Storage Systems are based on trusted computing platform technology. It uses a Trusted Platform Module (TPM), specified by the Trusted Computing Group in every storage node of the Cloud to build a trusted storage Cloud. The TPM is a special chip installed on the heart of a computer that performs basic cryptographic functions. It also stores the encrypted data within itself [2]. Some of the systems and modules are as:

3.1. Encrypted File System(EFS):

Encrypted File System meant for encrypting stored files. Encryption procedures are transparent to the user and are present at the user level not at the application level. These methods use cryptographic techniques for encrypting the various files automatically; hence user saves from cumbersome task of managing keys in encryption.

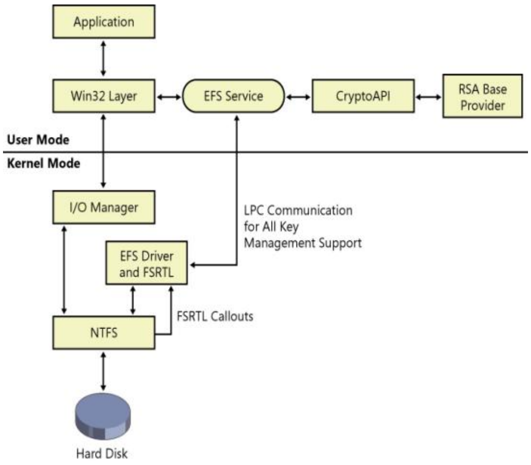


Fig 3: Encrypted file system in Microsoft Windows

Process explanatory steps are as follows as according in (see Figure 3):

- Data moves from application database to the NTFS driver.
- NTFS passes data to Input Output Manager, whose responsibility is to write data to the disk using NTFS.
- NTFS passes the data to EFS Driver which encrypts data and responds to NTFS with encrypted data and encryption/decryption keys.
- NTFS at last writes data and associated keys on the disk.

3.2. Trusted Platform Module (TPM)

TPM is a special chip on an endpoint device that stores RSA encryption keys called Endorsement Keys (E_k) as shown in Fig.4 specific to the host system for hardware authentication. That chip is provided by the Trusted Computing Group (TCG) [2]. For various parts of the module (see Figure 4).

This method is only applicable at administration level not at user level. If any modifications are being done then TPM detects it and thus shows the path how to proceed further to resolve it. It contains various Platform Configuration Registers (PCR'S) that allow secure storage and relevant security metrices. Thus to maintain integrity and confidentiality at storage systems it will be useful but at client's side we need some other techniques.

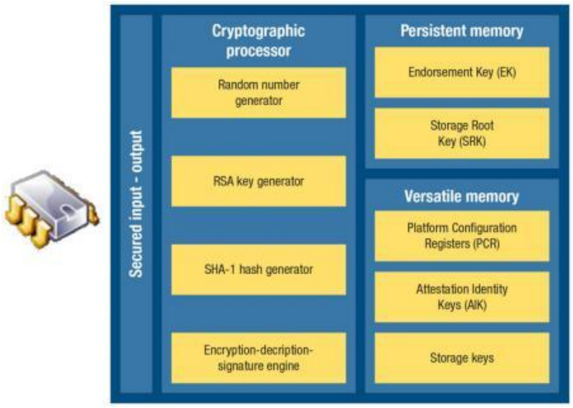


Fig 4: Steps involved in managing a TPM

3.3.Trusted Computing Group(TCG)

The prominent approach to Trusted Computing technology has been represented by the Trusted Computing Group (TCG). The TCG suggests elaborating all common platforms to coordinate between trusted components in software and hardware. It also secure, develop and promote the In particular the hardware extension known as Trusted Platform Module (TPM) which acts as a hardware trust anchor and allows to verify the integrity of the measured platform's software stack at load-time or boot time and reports to the remote party secretly and safely. Thus it supports the authenticated verifiability and transparency of a trusted platform's software state.

3.4. Trusted Network Connect(TNC)

Trusted Network Connect (TNC) architecture provides an industry standard approach to network security and Network Access Control (NAC) that works with leading providers such as Microsoft and Cisco. The Trusted Network Connect (TNC) Work Group has described and released an open architecture and a growing set of standards for endpoint integrity [6].

4. KERBEROS SERVICES

Here it is ensured that Cloud storage security must be authenticated at each level anyhow by any means. It is developed by MIT to protect network service from being corrupted or attacked. Kerberos is a great idea or say an approach provided to the user for the authentication of true source and destination. It authenticates credentials in either clear or hashed form without transferring a password. Thus offline password cracking becomes impossible. Kerberos supports single sign-on too. If anyone is logged on once then with the help of special ticket additional services can be enjoyed up also. If anyone access a Windows file server say, the file server will not bare if the logon credentials are sufficient. Under the cover, the authentication code automatically acquires a service ticket for the file server based on the logon ticket. It uses third party term for some type of authentication. Some of frequently used terms in this are as:

- KDC (Key Distribution Centre).
- AS (Authentication Server).
- TGS (Ticket Granting System).

Steps of authentication process as shown in (see Figure 5):

- Log on to workstation through the valid credentials by requesting through a ticket.

- 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 then access to the service.

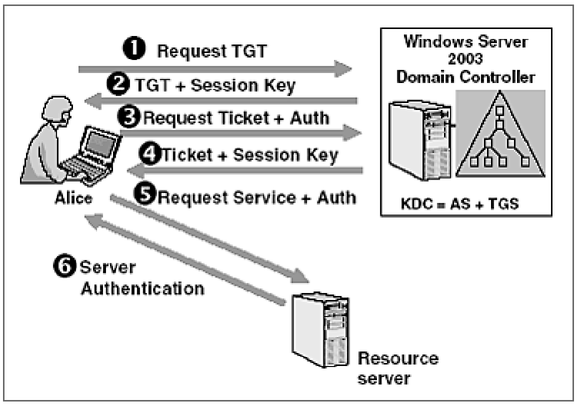


Fig 5: working of KERBEROS

Thus, Kerberos's authentication service allows the file system to be in authorised hands without any risk and failure.

5. AUDITING SERVICES

Some other methods like Service Level Agreements (SLA's) and Third Party Auditing (TPA) are also important to be taken into grant so as to secure the Cloud with double check and prevent from most type of attacks and risks.

5.1.Service Level Agreement(SLA):

SLA's are nothing but a contract between a service provider (either internal or external) and also describes the various services that can be accessed by the users. SLAs are output-based service that define their purpose is specifically to define what the customer will receive. SLAs do not define how the service itself is provided or delivered. The metrics that define levels of service for a SLA should aim to guarantee: reliability, responsiveness, monitoring and reporting problems. Though the exact metrics for each SLA vary depending on the service provider, the areas covered are uniform: volume and quality of work speed, responsiveness, and efficiency. In covering these areas, the document aims to establish a basic commitment of services in specific domains, responsibilities, guarantees, and warranties provided by the service provider.

5.2.Third Party Auditor (TPA):

The third party auditors are trusted experts which have the extra knowledge in relation with Cloud's data security and accessing it by keeping a check on behalf Cloud's user. These have the right to access dynamically over the Cloud Server for the regular updation and modifications. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA as shown in (see Figure 6)[13]. The benefit of delegating responsibility to trusted third party is that it reliefs the client from any kind of key management or over head is maintenance of any key information related to data on it device, because of which it allows the client to use any browser enabled devices to access such service[13]. We just trust the auditor who ensures quality and security being middleman between user and Cloud provider. TPA should efficiently work within ensured protocols without any deviation from the prescribed content.

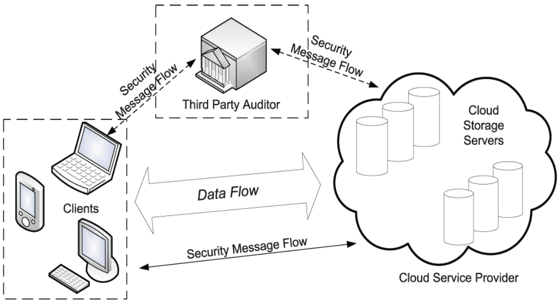


Fig 6: Involvement of THIRD PARTY AUDITOR in Cloud

6. CONCLUSION AND FUTURE WORK

In this paper it has been discussed about the various privacy and security issues in Cloud's data storage. Various encryption decryption algorithm with a trusted storage platform and an authentication service provided by Kerberos to the Cloud along with the verification of the SLAs and third party auditor were taken into consideration and also reached a conclusion that these are good for a simple Cloud storage system and will work efficiently for them but if moving towards a complex Cloud storage system at some level there would be more risk of security, integrity, confidentiality as well as privacy too. From the above survey it is cleared that as growing technologies along with the data storage requirements are increasing massively there should be some protocols or the type of algorithm that can keep a check on the various parameters of the security so that organisation can keep the data securely over the Cloud with trust. It will be an effective and trustworthy innovation in the field of Cloud which will enhance its capabilities and can be used freely. Thus, further in future the proposed modifications with efficient implementation of these and various other algorithms and authentication services for complex Cloud data storage systems will be presented.

7. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, N.Cao and W. Lou, "Towards Secure and Dependable data storage services in Cloud computing", in Proc. of IWQoS'09, July 2009.

[2] Sunita Sharma, Amit Chugh, "Survey Paper on Cloud Storage Security", IJIRCCE, Vol.1, Issue 2, April 2013, ISSN (online): 2320-9801.

[3] Ganesh Mouli Bandari, N. Subhash Chandra, V.Krishna, "Secure Cloud Storage through Public Auditing and Cryptographic Primitives", IJCTT-Vol.15, Number 2 – Sep 2014, ISSN: 2231-2803.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in Cloud computing", in Proc. of IWQoS'09, July 2009, pp. 1–9.

[5] Parsi Kalpana ," Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in

Computer and Communication technology, IJRCCT, ISSN:2278-5841, Vol 1, Issue 4, September 2012.

[6] Mr. Kailash Patidar ,Mr. Ravindra Gupta ,Prof. Gajendra Singh ,Ms.Megha Jain ,Ms.Priyanka Shrivastava, " Integrating the Trusted Computing Platform into the Security of Cloud Computing System", IJARCSSE, Vol.2, Issue 2, Feb 2012, ISSN: 2277 128X.

[7] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest", in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

[8] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila, IJCSIT, Vol. 2, ISSN: 1836-1840, 2011.

[9] Mehdi Hojabri, "Ensuring data storage security in Cloud computing with effect of Kerberos", Vol. 1 Issue 5, July – 2012, ISSN: 2278- 01 81.

[10] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents", Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

[11] S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn, "Virtualizing the trusted platform module", In Proc. of USENIX-SS'06, Berkeley, CA, USA, 2006.

[12] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", IJARCS, Vol. 2, No.6, Nov-Dec 2011.

[13] Balakrishnan.S , Saranya.G, Shobana.S, Karthikeyan.S, "Introducing effective Third Party Audting for data storage security in Cloud Computing", IJCST Vol.2, Issue 2, June 2011, ISSN: 0976-8491.

[14] Abha Sachdev and Mohit Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", IJCA, ISSN: 0975 – 8887, Vol. 67– No.9, April 2013.

[15] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of Cloud computing", 2009 IEEE Co Published by the IEEE Computer and Reliability Societies.