THIRD PARTY AUDITING FOR SECURE DATA STORAGE IN CLOUD THROUGH DIGITAL SIGNATURE USING RSA

K.Govinda[#1], V.Gurunathaprasad[#2], H.Sathishkumar[#3]

#1 SCSE,VIT University,8925467665
#2 SCSE,VIT University,9345017383
#3 SCSE,VIT University,7845368091

ABSTRACT

Cloud computing is the way of providing computing resources in the form of service rather than a product, utilities are provided to the users over internet. The main goal of cloud computing concept is to secure, protect the data and the processes which come under the property of users. The security of cloud computing environment is an exclusive research area which requires further development from both the academic and research communities. In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper we proposed digital signature method to protect the privacy and integrity of outsourced data in cloud environment.

.

Key words: Audit, Cloud, Signature, TPA, Data Integrity.

Corresponding Author: K.Govinda

INTRODUCTION

Cloud computing is foreseen to be the upcoming architecture to be employed in industries, owing to its vast merits in information technology history. Need for self-services, universal network processing of a network location autonomous resources availability, spontaneous resources flexibility, pricing is determined on the level of usage also on the risk of the transfer [4]. As a disarray invention with foreseen implication, cloud computing is mending way it uses business with IT. The basic point of view pattern is changing the way it is being focused over the cloud. In the view of users i.e. combining individuals and IT industries, storing the data remotely on cloud bring more benefits. Manual storage is completely lessened, We can access it universally with ubiquitous geographical location, The expenditure on hardware, software and personal maintenance is brought down [7]. In addition to this advantage it brings forth exclusive and challenging security threats towards user's outsourced data. Digital signature checks the proof of the sender or signer of the file ensuring that the contents are unchanged. This paper finds out the privacy implication of digital signatures.

Here the user has two keys, one of which only the owner knows called private key and another one which is known to anyone called public key. The knowledge of the public key in general doesn't threat the security. It is message digest that is created using the private key of the sender and the message digit again re-created using the public key of the sender we decrypt it here we match both the data it must be same as the sent one on the sender cannot deny that they sent it(non repudiation). As users don't possess the storage of data physically. We cannot follow the traditional cryptographic primitives for data security protection [3]. In general, the downloading of data for its integrity verification is impractical task since its very costly because of the transmission cost across the network. Identifying the data corruption only while accessing data is not enough, it must show the data corrupt even while not accessing it, which it doesn't and it might be very late to recover the damaged data. Taking into view that big amount of data is outsourced and the users constrained resource responsibility it's very expensive for the cloud user to check the data correctness in a cloud environment [5].

For well organization it is very essential that cloud that allows investigation from a single party. audit the outsource data to ensure the data security and save the user's computation and data storage. it is very important to provide public auditing service for cloud data storage, so that the user trust an independent third party auditor (TPA). TPA checks the integrity of data on the cloud on the behalf of the users, and it provides the reasonable way for the users to check the validity of data in the cloud. On the whole, enabling public auditing services plays a vital role in establishing cloud economy, where by users need way to assess to risk and gain faith in the cloud [6]. Public auditing in addition to user provides the external party to verify the correctness of stored data against the external attacks. However these schemes [1], [5], [2] don't involve the privacy protection of the data. It is a main disadvantage which affect the security of the protocols in cloud computing. So the users who depend on TPA only for their security storage want their data to be protected from the external auditors. i.e. they focus that there is no leakage of data security [8]. Also there are US Health Insurance Portability and Accountability act(HIPAA)which are on demand because they assure that data is not available to the external parties.

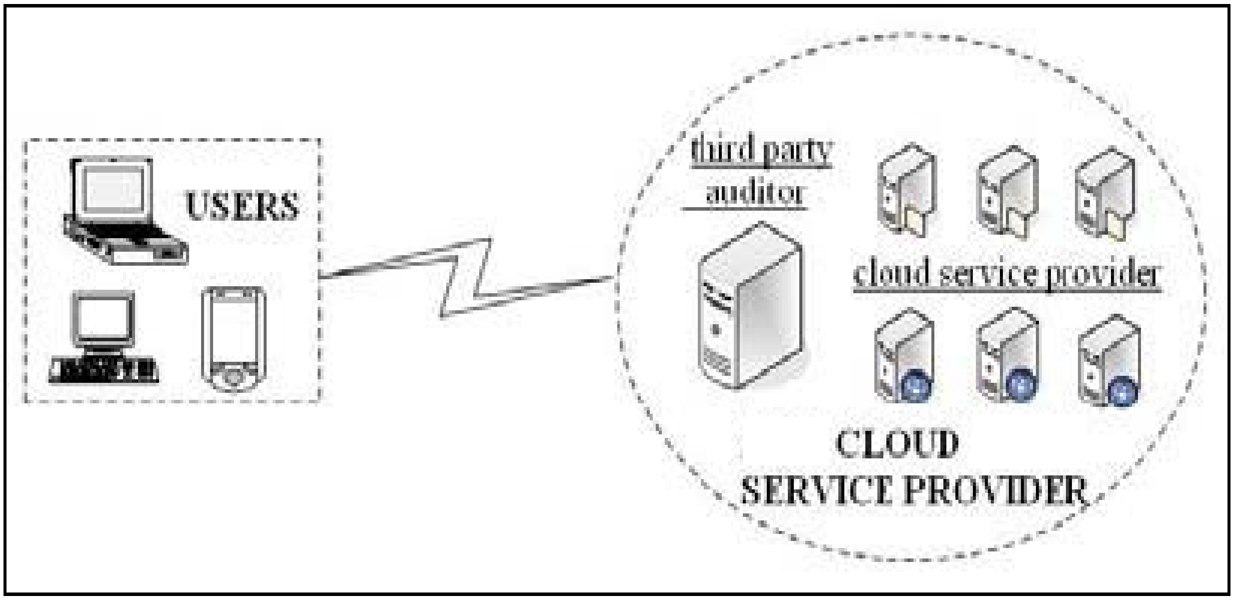


Figure1. TPA with Service Provider

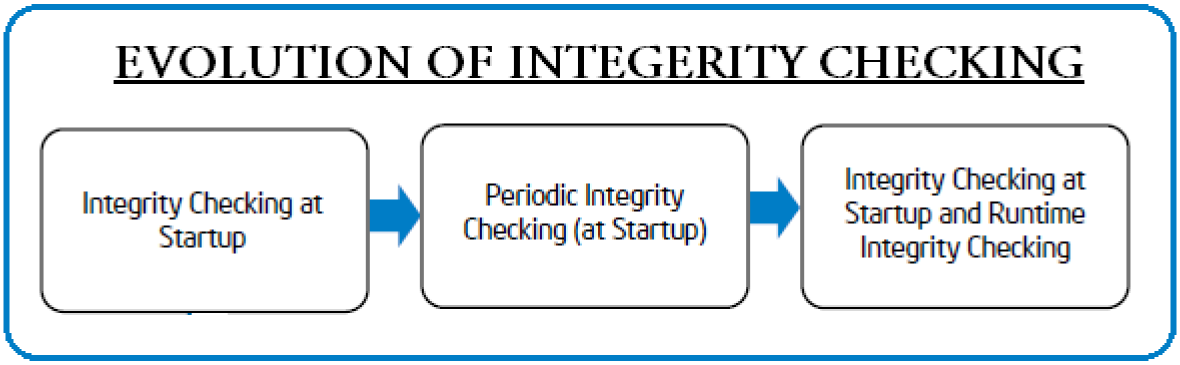
Users are active participants. They have data to be stored in the cloud and rely on the cloud for data maintenance and computation. Both individual consumers and organizations can be the users. Cloud service provider has significant storage space and computation resource to maintain the users' data. It also has expertise in building and managing distributed cloud storage servers and the ability to own and operate live cloud computing systems. Third party auditor has expertise and capabilities that users do not have and it is trusted to assess and expose risk of cloud storage services on behalf of the users upon request. Similar to [7], users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and security. Users should be equipped with certain security means so that they can make sure their data is safe. Cloud service provider is always online and assumed to have abundant storage capacity and computation power. The third party auditor is invariably online, too. It makes every data access be in control. In this paper, we proposed a model for cloud storage and auditing using digital signature.

MATERIALS AND METHODS

Cloud computing is nowadays evolving as a revolution. In cloud computing, cloud security is one of the most challenging task. Cloud computing entrusts services with users data, software and computation on a published application programming interface over a network. The cloud provides a platform for many types of services. It has a considerable overlap with software as a service (SaaS) [2]. End users access cloud based applications through a web browser or a light weight desktop or a mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance than if the software programs were installed.

When we talk about cloud Security, maintaining data integrity is one of the most important and difficult task. When we talk about cloud users, they are using cloud services provided by the cloud provider [2]. Again, in case of maintaining the integrity of the data, we cannot trust the service provider to handle the data, as he himself can modify the original data and the integrity may be lost. If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider . So, in this case ,we take the help of a trusted third party auditor to check for the integrity of our data. This third party auditor takes care of our data and makes sure that the data integrity is maintained.

We view the procedure of integrity checking as a key's proficiency within the software, platform, and infrastructure security focus area of our cloud architecture. Our vision for helping assure ongoing system integrity in a virtualized environment includes an evolution of integrity-checking competences [2]. Each phase in this evolution provides an increasing level of assurance and relies on secure startup enabled. This evolution begins with one-time integrity checks at system or hypervisor startup, progresses to more frequent periodic integrity checks, and terminates in runtime integrity checks. In a traditional computing environment, increasing restart frequency is difficult because applications are tied to physical servers; restarting a production server can result in unacceptable application downtime [2].


EVOLUTION OF INTEGERITY CHECKING
Integrity Checking at Startup
Periodic Integrity Checking (at Startup)
Integrity Checking at Startup and Runtime Integrity Checking

Data integrity can be assured by quite a lot of ways. Online integrity checks help to identify and in some cases make good progress from integrity violations. Some systems, instead of performing checks for Integrity, employ preventive methods to reduce the likelihood of an integrity violation [1]. In this section we classify integrity assurance mechanisms into three main types, based on their goals:

1. Those that perform defensive steps so as to avoid exact types of integrity damages;
2. Those that perform integrity checks and detect integrity violations;
3. Those that is skilled of improving from loss once a violation is detected.

The check summing techniques helps in detecting integrity violations. They generally cannot help recovery for two reasons [4]. First, a mismatch between the stored value and the computed value of the checksums just means that one of them was modified, but it does not provide information about which of them is legitimate [3]. Stored checksums are also likely to be modified or corrupted. Second, checksums are generally computed using a one-way hash function and the data cannot be reconstructed given a checksum value.

In proposed method we use RSA algorithm for encryption and decryption which follows the process of digital signature for the message authentication. In our protocol there are three main participants. As discussed above (i) Third Party Auditor (TPA) (ii) User (iii) Cloud Provider. As the initial requirement the user and the TPA generates their own private key and public key with respect to the strong RSA algorithm. The public keys have been shared between them as the part of SLA or in some other ways. Then with respect to the protocol the message is encrypted as well as signed in a unique way.

With Respect to the RSA Algorithm, the user selects two relative prime number p1 and q1with these, the following values are computed.

$n1 = p1 * q1$

$fn1 = (p1-1) * (q1-1)$

Then, the public key $\alpha 1$ is selected.

So, the Private Key of the TPA

$\beta 1 = (1/\alpha 1) \% fn1$

Similarly, the user selects his own relative prime numbers p2 and q2 with these the private key and the public key of the user is estimated as,

$n2 = p2 * q2$

$fn2 = (p2-1) * (q2-1)$

The public key of the user is declared as $\alpha 2$

So, the Private Key of the user is,
$\beta 2 = (1/\alpha 2) \% fn2$

Now, Key set of TPA is : $\{\alpha 1, n1\},\{\beta 1, n1\}$
Key set of User is : $\{\alpha 2, n2\},\{\beta 2, n2\}$

With the generated public key sets they get exchanged between the user and the TPA. At first the data is signed with the user's private key then the cipher is again encrypted with the TPA's public key. This package is now sent to the Cloud and also the TPA.

Data encrypted form is: $\{\{\{data\}\beta 2\}\alpha 1\}$.

The TPA now decrypts the encrypted message with his private key and then de-signs the cipher with the user's public key to recognize the data. Then the same process of decryption is carried out in the cloud by the TPA to verify the correctness by comparing the data which he has with the stored one. Then as per the result the TPA indicates the user.

CONCLUSION

In this paper we proposed provably secure auditing protocol to store data and verify it. We used RSA algorithm for digital signature and for the process of encryption and decryption this can also be designed with some other algorithms or tool.

REFERENCE

[1] Q.Wang ,C.Wang, j.Li, K.Ren, and W.lou, “Enabling public verifiability and data dynamics for storage security in cloud computing”.

[2] H.shacham and b.waters “compact proofs of retrivability “in proc. Of asiascrypt 2008.

[3] P.Mell and T,Grance, “Draft NIST working definition of cloud computing”, referred on june 3rd 2009.

[4] M.AShah,R.Swaminathan, and M.Baker"privacy-preserving audit and extraction of digital contents".

[5] Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.H.Katz,A.Konwinski, G.Lee, D.A.Patterson ,A.Rabkin,I.Stoica, and M.Zaharia,"Above the clouds:A Berkeley view of cloud computing", feb 2009

[6] M.A.Shah,M.Baker,J.C.Mogul, and R.swaminathan, "Auditing to keep online storage services honest",in Proc.of hotOS'07.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,"Enabling Public Verifiability and Data Dy_ _namics for Storage Security in Cloud Computing," Proc. 14th European Symp. Research in Computer Security (ESORICS '09), pp. 355-370, 2009