IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud

Reshu Tomar[1], Rajkumar Singh Rathore [2]

Dept. of Computer Science, Galgotia College of Engineering and Technology, Greater Noida, India[1]

Assistant Professor, Dept. of Computer Science and Information Technology,

Galgotia College of Engineering and Technology, Greater Noida, India[2]

Abstract: Cloud Computing is that the new buzz word in today's computing world. though there's large buzz, many of us are confused on specifically what cloud computing is, particularly the term is used to mean nearly anything. Cloud Computing has been visualised because the next generation design of IT Enterprise. It moves the application software and databases to the centralized massive data centres, wherever the management of the data and services might not be absolutely trustworthy. This distinctive paradigm brings concerning several new security challenges, that haven't been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. Especially, we think about the task of permitting a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data kept within the cloud. To securely introduce an efficient third party auditor (TPA), the subsequent two basic necessities should be met. First, TPA should be able to efficiently audit the cloud data storage without demanding the native copy of data, and introduce no extra on-line burden to the cloud user. Second, the third party auditing method should bring in no new vulnerabilities towards user data privacy. During this paper, we utilize and uniquely combine the general public key primarily based homomorphic authenticator with random masking to realize the privacy-preserving public cloud data auditing system, which meets all above needs. to deal with these issues, our work utilizes the technique of secret key primarily based bilaterally symmetrical key cryptography that enables TPA to perform the auditing without demanding the native copy of user's keep data and therefore severely deduces the transmission and computation overhead as compared to the simple data auditing approaches. The projected system offer safer design by using light weighted APCC (Authentication protocol for cloud computing).In previous system SSL is employed for this purpose. Than challenge handshake authentication protocol is employed for authentication. Challenge handshake authentication protocol is employed for authentication once client request for any data or service on the cloud .We will use VerifyProof run by TPA to audit the proof from the cloud. Initially request sends for identity of client by Service supplier authenticator. For sending or receiving data over cloud we are going to use blowfish for security purpose.

Keywords: Cloud computing, Cloud, TPA, Cryptography, Blowfish, symmetric key.

I. INTRODUCTION

Cloud Computing that provides internet based mostly service and use of technology. This is often cheaper and a lot of robust processors, along with the software as a service (SaaS) computing architecture, are remodelling information into data centres on large scale. The increasing network and versatile network connections build it even potential that users will currently use prime quality services from data and provides remote on data centers. Storing data into the cloud offers nice facility to users since they don't need to care regarding the issues of hardware problems. Whereas these internet-based on-line services do offer large amounts of space for storing and customizable computing resources, this computing platform shift, however, it avoids the responsibility of native machines for data maintenance simontaneously. As a result, users are at the interest of their cloud service providers for the availability and integrity of their data at one hand; though the cloud services are far more powerful and reliable than personal computing devices and broad vary of each internal and external threats for data integrity still exist. Samples of outages and data loss incidents of noteworthy cloud storage services seem from time to time. On the opposite hand, since users might not keep a neighbourhood copy of outsourced data; there exist numerous incentives for cloud service providers (CSP) to behave unreliably towards the cloud users relating to the status of their outsourced data. Our work is among the primary few ones during this field to think about distributed data storage security in Cloud Computing. Our contribution is summarized because the following three aspects:

1) We encourage the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our system allows an external auditor to audit user's cloud data while not learning the data content.
2) To the best of our information, our approach is the initial to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, our approach achieves batch auditing wherever multiple delegated auditing tasks from totally different users may be performed at the same time by the TPA during a privacy-preserving manner.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

3) We prove the safety and justify the performance of our projected schemes through concrete experiments and comparisons with the state-of-the-art.

Fig 1.1: Cloud Architecture

II. SYSTEM MODEL

Third Party Auditor (TPA)

We take into account a cloud data storage service involving three completely different entities, as illustrated in Fig. 1.2, the cloud user, who has large amount of data files to be stored within the cloud; the cloud server (CS), that is handled by the cloud service provider (CSP) to provide data storage service and has vital space for storing and computation resources .we won't differentiate between CS and CSP thereafter; the third party auditor (TPA), who has expertise and abilities that cloud users don't have and is trustworthy to assess the cloud storage service reliability on behalf of the user upon request. Users have faith on the CS for cloud data storage and maintenance. They'll also dynamically interact with the CS to access and update their stored data for numerous application purposes. As users now not possess their data locally, it is of vital importance for users to make sure that their data are being properly stored and maintained. to save lots of the computation resource as well as the on-line burden potentially brought by the periodic storage correctness verification, cloud users might resort to TPA for guarantee the storage integrity of their outsourced data, whereas hoping to keep their data private from TPA. We tend to assume the data integrity threats towards users' data can come from each internal and external attacks at cs. These could include: package bugs, hardware failures, bugs within the network path, economically driven hackers, malicious or accidental management errors, etc. Besides, CS may be self-interested. For their own benefits, like to maintain reputation, CS may even attempt to hide these data corruption incidents to users. Using third-party auditing service provides an economical technique for users to realize trust in Cloud. For well organization it's very essential that cloud that enables investigation from one party audit the outsource data to assure data security and saves the user's computation and data storage [3], [4]. It's vital to provide public auditing service for cloud data storage, so the user has faith in an independent third party auditor (TPA) [5]. TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable means for users to ascertain the validity of data in cloud [6]. We tend to assume the TPA, who is within the business of auditing, is reliable and independent. However, it may harm the user if the TPA could learn the outsourced data after the audit.

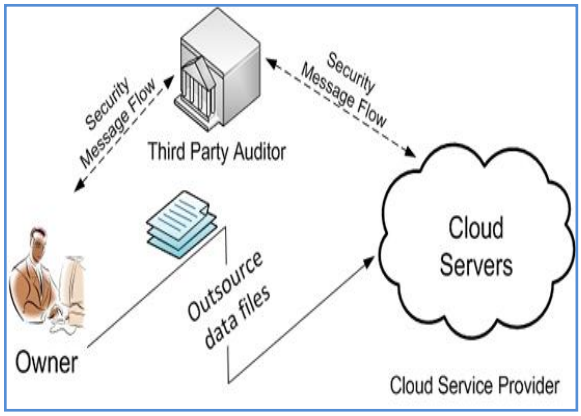

Fig. 2.1 Third Party Auditor

III.DRAWBACKS OF EXISTING SYSTEM

Security in cloud has become the most on crucial issue to be addressed in cloud computing environment.

- With the help of cloud user become free from different data management task, as this data management is handelled by the third party expert auditor (TPA). But still there are certain security issues of this third party auditor as during this audit TPA can get access to the data in the cloud.
- Cloud services are also gives users' physical control of their outsourced data, which provides control over security problems towards the correctness of the storage data in the cloud.
- The integrity of data in cloud storage, however, is subject and matter to skepticism and scrutiny, as data stored within the cloud can easily be lost or corrupted because of the inevitable hardware/software failures and human errors [1], [2].
- The third party Auditor (TPA), cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request.
- Since users may not keep a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data

IV. DESIGNS GOALS

To enable privacy-preserving public auditing for cloud data storage below the mentioned model, our protocol design should reach the subsequent security and Performance guarantees.

- **Public audit ability**: To allow TPA to verify the correctness of the cloud data on demand while not retrieving a copy of the total data or introducing further on-line burden to the cloud users.
- **Storage correctness**: To ensure that there exists no cheating cloud server that may pass the TPA's audit without indeed storing users' data intact.

DOI 10.17148/IARJSET.2016.3419

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

- **Privacy-preserving**: To confirm that the TPA cannot derive users' data content from the information collected throughout the auditing method.
- **Batch auditing**: To enable TPA with secure and efficient auditing capability to deal with multiple auditing delegations from possibly large number of various users at the same time.
- **Lightweight:** To permit TPA to perform auditing with minimum communication and computation overhead.

V. PROPOSED METHODOLOGY

To achieve privacy preserving public auditing we proposed a solution for TPA by three way handshaking by Extensible Authentication Protocol (EAP) with advanced encryption standard .The proposed system provide more secure Architecture by using light weighted APCC(Authentication protocol for cloud computing).In previous system SSL is used for this purpose. Than challenge handshake authentication protocol is used for authentication. Challenge Handshake authentication protocol is used for authentication when client request for any data or service on the cloud .We will use Verify Proof run by TPA to audit the proof from the cloud. First request sends for identity of client by Service provider authenticator. For sending or receiving data over cloud we will use blowfish for security purpose.

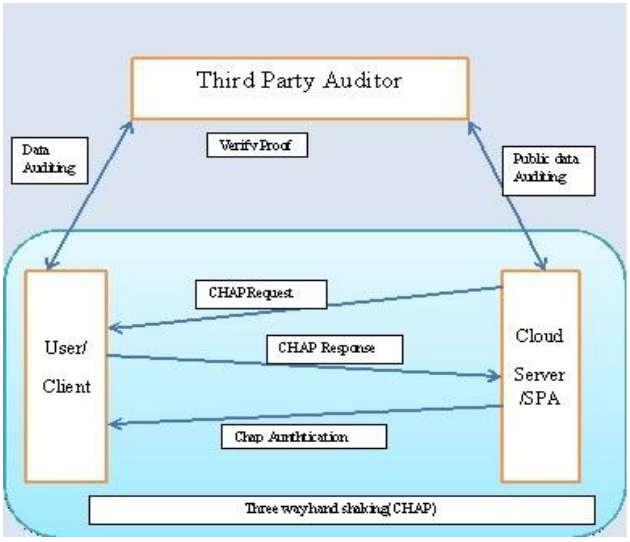

Fig. 4.1 Proposed System Model

VI. MOTIVATION

Blowfish

Blowfish is a bilaterally symmetrical block cipher that may be effectively used for encryption and safeguarding of data. It takes a variable-length key, from thirty two bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a quick, free alternative to existing encryption algorithms. Since then it's been analyzed significantly, and it is slowly gaining acceptance as a powerful encryption algorithm. Blowfish is nonproprietary and license-free, and is accessible free for all uses. Blowfish algorithm is a Feistel Network, iterating a straightforward encryption perform sixteen times. The block size is sixty four bits, and also the key may be any length up to 448 bits. Though there's a complex initialization part needed before any encryption will occur, the particular encryption of data is extremely efficient on massive microprocessors. Blowfish may be a variable-length key block cipher. It's appropriate for applications wherever the key doesn't modify usually, sort of a communications link or an automatic file encryption. It's considerably quicker than most encryption algorithms once implemented on 32-bit microprocessors with massive data caches. Blowfish could be a symmetrical block encryption algorithmic program designed in consideration with:

- Fast: It encrypts data on massive 32-bit microprocessors at a rate of 26 clock cycles per byte.
- Compact: It can run in less than 5K of memory.
- Simple: It uses addition, XOR, lookup table with 32-bit operands.
- Secure: The key length is variable, it may be within the range of 32~448 bits , default 128 bits key length.

Blowfish symmetrical block cipher algorithm that encrypts block data of 64-bits at a time. It'll follow the feistel network and this algorithm is split into two parts.

1. Key-expansion
2. Data encryption

Key-expansion:

It'll convert a key of at the most 448 bits into many sub key arrays totaling 4168 bytes. Blowfish uses large number of sub keys. These keys are generating earlier to any data encryption or data decryption.

The p-array consists of 18, 32-bit sub keys:
P1, P2,……., P18

Four 32-bit S-Boxes incorporate 256 entries each:
S1,0, S1,1,……. S1, 255
S2,0, S2,1,…….. S2, 255
S3,0, S3,1,…….. S3, 255

In total, 521 iterations are needed to generate all required sub keys. Applications can store the sub keys instead of execute this derivation method multiple times.

Data Encryption:

It is having a function to iterate sixteen times of network. Every round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for every round. Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of 2 halves: a key-expansion half and a data- encryption part. Key expansion converts a key of at the most 448 bits into many sub key arrays totaling 4168 bytes. Data encryption happens via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key- and data-dependent substitution.

Algorithm: Blowfish encryption
Step 1: Divide x into two 32-bit halves: xL, xR
Step 2: For i = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR

DOI 10.17148/IARJSET.2016.3419

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 4, April 2016

Step 3: Swap XL and xR
Step 4: Swap XL and xR (Undo the last swap.)
Step 5: xR = xR XOR P17
Step 6: xL = xL XOR P18
Step 7: Recombine xL and xR

Feistel Networks
A Feistel network is a general methodology of transforming any function (usually referred to as an F function) into a permutation. It absolutely was fabricated by crust Feistel and has been employed in several block cipher technique.

The functioning of a Feistal Network is given below:

- Split every block into halves
- Right half becomes new left half
- New right half is that the end result when the left half is XOR'd with the results of applying f to the right half and also the key.
- Note that previous rounds are often derived even though the function f isn't invertible.

Table 1: Comparison results using Crypto++

Algorithm	**MB(2^20 bytes)**	**Time Taken**	**MB/Sec**
Blowfish	256	3.976	64.386
Rijndael (128-bit key)	256	4.196	61.010
Rijndael (192-bit key)	256	4.817	53.145
Rijndael (256-bit key)	256	5.308	48.229
Rijndael (128) CTR	256	4.436	57.710
Rijndael (128) OFB	256	4.837	52.925
Rijndael (128) CFB	256	5.378	47.601
Rijndael (128) CBC	256	4.617	55.447
DES	128	5.998	21.340
(3DES)DES-XEX3	128	6.159	20.783
(3DES)DES-EDE3	64	6.499	9.848

VII.CONCLUSION

In this paper, we have provided the mechanism for trusted and secure data storage model with new scheme by using Blowfish encryption algorithm with integrity verification. The features of algorithm are useful to reduce computational cost for the client who may not have much security processing power. Using TPA we can audit the data on the server, and can preserve the privacy in data communication. Thus we can secure our data on the cloud servers using this Mechanism. Third Party Auditor are often accustomed make sure the security and integrity of data. Third party auditor is often a trustworthy third party to resolve the conflicts between the cloud service provider and also the client. This scheme is proposed to provide a trustworthy atmosphere for cloud services.

VIII. FUTURE WORK

Cloud Computing is a vast concept and security plays a very important role in case of Clouds. There is a huge scope of improvement in this area. Future work is planned to provide higher level of security by implementing Blowfish encryption algorithm for cloud services.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no.1 pp. 69-73, 2012.
[2] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.
[4] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop(CCSW'10), pp. 31-42, 2010.
[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security(ESORICS'09), pp. 355-370, 2009.
[6] Farzad Sabahi,"Cloud Computing Security Threats and Responses" ,IEEE confer. 2011, 978-1-61284-486-2/111