ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

TPA BASED CLOUD STORAGE SECURITY TECHNIQUES

ANUPRIYA.A.S, ANANTHI, Dr. S KARTHIK

***Abstract*-Cloud Computing is the new trend to reduce the investment in business to satisfy the client needs using internet. The various cloud services provides infrastructure, software and platform. In cloud computing, data is moved to a remote location. Users store their data conscientiously in the cloud and return back when it is needed. But there is no assurance for the data stored in the cloud is secure and not changed by the cloud or Third Party Auditor (TPA).Users should be able to assist the TPA to overcome the integrity problems in cloud. In this paper, an enhanced method for securing the TPA by using Keyed Hash Message Authentication Code (HMAC) is proposed.**

***Keywords*-Security, Cloud Storage, Third party auditors, Cloud computing, cloud server**.

I.INTRODUCTION

Cloud computing is a method in which computing power, memory, infrastructure can be delivered as a service. A Cloud computing is a set of network enabled services, guaranteed QoS, inexpensive computing infrastructures on demand with an easy and simple access. Cloud security is an evolving sub-domain of computer security, network and information security [8]. Security in cloud can be implemented remotely by client where the data centres and protocols in the security objectives of the service provider are: i) confidentiality for securing the data access and transfer ii) auditability for checking whether the security aspect of applications has been tampered or not. Dimensions of cloud security have been aggregated into three areas like security and privacy, compliance and legal issues.

II. CLOUD SERVICES

A.Cloud software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The application is accessible from various client devices through web browser.

B.Cloud platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application created using programming languages and tools supported by the provider.

C. *Cloud infrastructure as a service (IaaS): The* capability provided to the consumer is to provision processing, storage, network and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating system and application

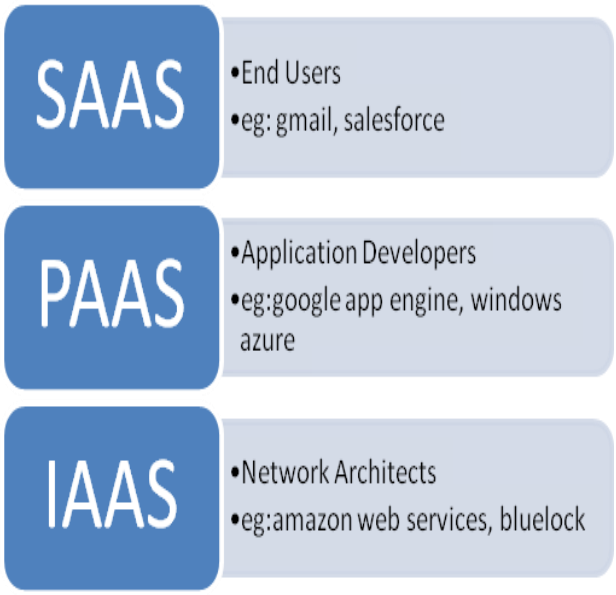

Fig 1: Cloud services

III.CHARACTERISTICS OF CLOUD COMPUTING

Cloud Computing includes 4 basic characteristics:

a. On-demand self service: Computing capabilities can be provisioned to the consumers.

b. Broad network access: Capabilities are present in the network which can be accessed through standard mechanisms.

c. Resource pooling: The provider's computing resources are pooled to serve multiple consumers with different physical and virtual resources dynamically assigned and reassigned according to the demand of consumer.

d. Rapid elasticity: Capabilities which allows rapid and elastic provisioning.

e. Measured service: Cloud systems which automatically control and optimize resource usage with a metering capability at some level of abstraction according to the type of service.

IV. BENEFITS OF CLOUD COMPUTING

The Advantages of Cloud Computing are:

Reduced cost: Cloud technology is paid incrementally which saves the money of organization.

Increased Storage: Comparing to a private computer systems more data of organization can be stored.

Manuscript received Sep 15, 2012.

Anupriya.A.S, *M.E Computer Science and Engineering, Anna University/SNS College of Technology, Coimbatore-641035,Tamil Nadu(email:anupriyas191@gmail.com),India ,8870793165*

S.Ananthi, *Computer Science and Engineering, Anna University/SNS College of Technology, Coimbatore-641035, Tamil Nadu (email id:aananthi_s@yahool.com), ,India,9843021703.*

S.Karthik*, Computer Science and Engineering, Anna University/SNS College of Technology, Coimbatore-641035, Tamil Nadu (e-mail:profskarhtik@gmail.com).*

Highly Automated: No longer have the IT personnel needed to be worry about keeping software up to date.
Flexibility: It provides much more flexibility than past computing methods.
More Mobility: Employees can access the information from anywhere rather than having to remain at their desks.
Allows IT to Shift Focus: No constant server updates and other computing issues, government will be free to concentrate on innovation.

V. SYSTEM MODEL

- User or client: an entity, who has data to be stored in the cloud.
- Cloud server (CS): an entity, which is guided by Cloud Service Provider (CSP) to provide data storage services.
- Third Party Auditor (TPA): an entity, which has adequacy and expertise to access and expose the risk of cloud storage services on behalf of users upon request.

VI. RELATED WORK

A. EFFICIENT INTEGRITY CHECKING TECHNIQUE

One of the major problem affecting the cloud computing is the integrity [4] of the cloud data. The threads of the data can overcome by using the assistance of a TPA. Introducing a model for checking the integrity over the cloud computing with the support of TPA using Digital Signature Technique.Fig.1 shows the architecture.

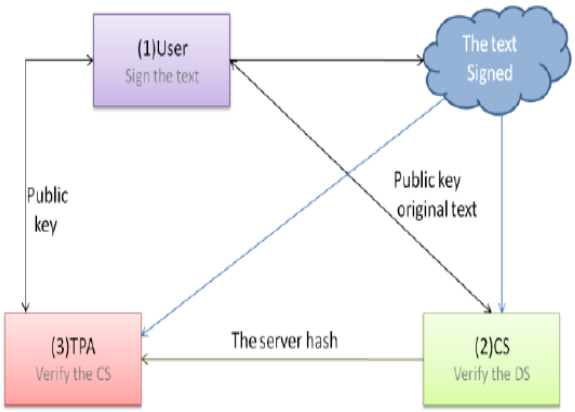

Fig.2: The Architecture of data integrity checking in cloud

The checking is performed over two parts: the cloud service provider (CSP) and TPA without giving any secure data.The Digital Signature first takes the user data and performs a hash function using Message-Digest Algorithm (MD5) [9]. For the generated hash value computes the signature by encrypting it with private key. On the other side decryption can be performed by the public key which contains a hash value in the reversible order of its original data.

B. STORAGE SECURITY AND PUBLIC AUDITABILITY

Users rely on the cloud server (CS) for cloud data storage and maintenance. They may interact with the CS to access and update their stored data for various applications. The Third Party Auditor (TPA) eliminates the auditing of client to check where his data is stored in the cloud. Since the services in cloud computing are not limited to data backup ,so the dynamic support of data such as block modification, insertion and deletion is significant [11]. The previous works lacks the support of either public auditability or dynamic data operations, where it achieves the both with remote data integrity.

It first identifies the security problems and difficulties of direct extensions with full dynamic data updates from the prior works and then shows how to construct a verification scheme for the integration. By manipulating the classic Merkle Hash Tree construction for block tag authentication the efficiency of data dynamics can be achieved. To support efficient handling of multiple auditing tasks, the technique of bilinear aggregate signature to extend the result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

C. PRIVACY-PRESERVING PUBLIC AUDITING

The Security problems in cloud computing creates the burden to the local data storage and maintenance. By utilising public auditability [2] the users can resort to an external audit party to the integrity of outsourced data when needed.

The auditing process by the TPA should not bring any new vulnerabilities towards user data privacy and should not increase the burden of the user .To overcome these disadvantages and to introduce a secure cloud storage with a auditing [5].

The main task is to guarantee that the TPA should not learn any knowledge about the content of data stored on cloud server during the auditing process, can be achieved by using the homomorphic non-linear authenticator and random masking [14]. By using privacy preserving public auditing should achieve the following design goals:

Public audit: The correctness of the cloud data can be verified by the TPA without retrieving the copy of the data.
Storage Consistency: The data, which is in the cloud server, will pass the audit from TPA without storing it.
Privacy preserving: It must guarantee that there is no way to get user's data content from the collected information.
Batch auditing: Provide TPA with secure and efficient auditing ability with multiple auditing delegations.

D. PUBLIC AUDITABILITY AND DATA DYNAMICS FOR STORAGE SECURITY

In cloud storage users will no longer posses the local copy of the outsourced data after storing the data. So the client should verify the integrity of the data stored in the remote entrusted server. To overcome these problems a remote integrity checking protocol [10].

This protocol is suitable for providing integrity protection of cloud data. It also supports data insertion, modification, and deletion at the block level with the support of public verifiability.

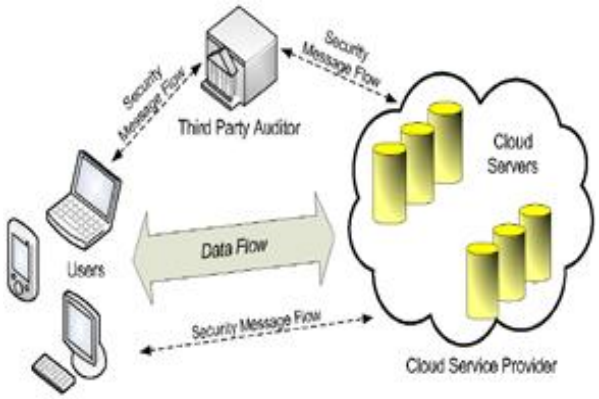

Fig. 3: The architecture of cloud data storage service

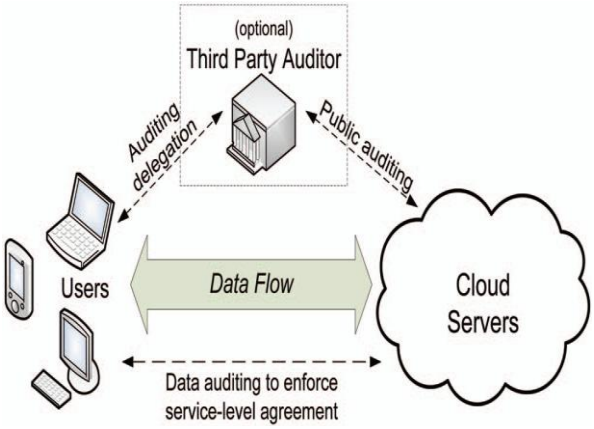

Fig.7: cloud storage service architecture.

Public verifiability provides client to verify the integrity task to TPA while they themselves can be unreliable or not able to commit necessary computation resources with continuous verifications. It is proved to secure against an untrusted server [1] and private against third party verifiers.

E.SECURE AND DEPENDABLE STORAGE SERVICE

The physical possession of the outsourced data creates new security risks in the cloud computing storage. This paper provides a secure TPA based storage utilising homomorphic token and distributed erasure coded data[8] which allows users to audit the cloud storage with very light weight communication and computation cost. The auditing results in strong cloud storage correctness guarantee and fast data error localization [16].

To ensure the dynamic nature of the cloud data, the proposed design supports secure and efficient dynamic operations on outsourced data including block modification, deletion and append. The analysis shows the efficiency and resilient against Byzantine failure, malicious data modification attack and server colluding attacks.

To provide redundancy parity vectors and guarantees data dependability using erasure-correcting code in the file distribution preparation [15]. Utilizing the homomorphic token and distributed verification of erasure coded data helps to achieve the integration of storage correctness insurance and data error localization. The advantages of dynamic data verification are

Storage correctness: Ensuring the user's data are stored appropriately and kept intact all the time in the cloud.

Fast localization of data error: Malfunctioned server can be easily located during data correction.

Dynamic data support: The same level of storage correctness assurance during user's modification, deletion or append the data files in the cloud should be maintained.

Dependability: Enhance data availability against Byzantine failures, malicious data modification and server colluding attacks.

Light weight: Perform storage correctness checking's with minimum overhead

VII. EXISTING SYSTEM

To introduce a efficient TPA for both security and privacy of cloud data It should met some fundamental requirements: the cloud data must be audit by the TPA without demanding local copy of data and reducing the online burden of the users.

All the above related works reveals the problem in providing security to the TPA caused due to various auditing protocols like public auditing, privacy preserving public auditing. In the existing model, provides a secure TPA based storage utilising homomorphic token and distributed erasure coded data [8] which allows users to audit the cloud storage with very light weight communication and computation cost. The auditing results in strong cloud storage correctness guarantee and fast data error localization.

VIII. PROPOSED SYSTEM

TPA ensures the correctness of data and allows the cloud client, to verify the integrity of the data stored in the cloud. The leakage of the user's outsourced data from the auditing protocol makes security and integrity problems in the cloud. Security to the TPA should provided by using hash function such as HMAC.

A HMAC function is used by the message sender to produce a value that is formed by condensing the secret key and the message input [3]. HMAC can be used with any iterative key and the message input. For the calculation of HMAC the hash function, such as MD5 or SHA1 can be used. The strength of the HMAC depends upon the strength of the hash function, size of the hash output length and size and quality of the key.

IX.CONCLUSION

In the cloud data storage, users store their data and no longer posses the data locally. In the distributed cloud servers, the correctness and availability of the data files being stored. One of the key issues is to effectively detect any unauthorized data modification and corruption. The Third Party Auditing allows to save the time and computation resources with reduced online burden of users. Security for the TPA can be provided by HMAC along with homomorphic tokens and erasure coded data.

ACKNOWLEDGMENT

The authors would like to thank the Editor in chief,the Associate Editor and anonymous Referees for their comments

REFERENCES

[1] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 598–609

[2]. Ateniese G, Pietro R.D, Mancini L.V, and Tsudik G, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New York, NY, USA: ACM, 2008, pp.1-10.

[3] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, andP. Rogaway. UMAC: Fast and secure message authentication.In *CRYPTO*, volume 1666 of *LNCS*, pages 216–233, 1999.

[4] Bowers K.D, Juels A, and Oprea A, "Hail: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09. Chicago, IL, USA: ACM, 2009, pp. 187–198.

[5] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Trans. Computer Systems, vol. 20, no. 4,pp. 398-461, 2002

[6] Chang E.C, and Xu J, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.

[7] Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing environments," *in Proceedings of Natural Sciences and Engineering*, Sweden, pp. 2-4, 2010.

[8] Cong Wang,Qian Wang,Kui Ren Ninig Cao and Wenjing Lou"Towards Secure and Dependable storage services in cloud computing",IEEE Transaction on service computing,vol 5,no 2,june 2012

[9] Dalia Attas and Omar Batrafi " Efficient integrity checking technique for securing client data in cloud computing", October 2011

[10] Jaison Vimalraj.T,M.Manoj"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", March2012

[11] Kayalvizhi S,Jagadeeswari "Data Dynamics for Storage Security and Public Auditability in Cloud Computing", February 10, 2012

[12] Metri P. and Sarote G., "Privacy Issues and Challenges in Cloud computing," *International Journal of Advanced Engineering Sciences and Technologies*, vol. 5, no. 1, pp. 5-6, 2011.

[13] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012

[14] D. Srinivas "Privacy-Preserving Public Auditing In Cloud Storage Security", November 2011

[15] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing tokeep online storage services honest," in *Proc. Of HotOS'07*., CA, USA: USENIX Association, 2007, pp. 1–6.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality ofService (IWQoS '09), pp. 1-9, July 2009

Anupriya.A.S received BE degree in Computer Science and Engineering from Anna University of Technology, Coimbatore, India in 2011.She is presently doin ME Computer Science and Engineeringin Anna University, Chennai from SNS College of Technology.Her area of interests is Cloud Computing.

S.Ananthi received MCA degree from Bharthidasan University Trichi, in 2003 and M.E degree in Computer Science and Engineering from Anna University,Coimbatore, India in 2011. She is at present working as Assistant Professor in the department of Computer Science Engineering at SNS College of Technology, Coimbatore, India. Her area of interest include Cloud Computing and Mobile Computing

Professor Dr.S.Karthik is presently Professor & Dean in the Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University- Coimbatore, Tamilnadu, India. He received the M.E degree from the Anna University Chennai and Ph.D degree from Ann University of Technology, Coimbatore. His research interests include network security, web services and wireless systems. In particular, he is currently working in a research group developing new Internet security architectures and active defense systems against DDoS attacks. Dr.S.Karthik published more than 35 papers in refereed international journals and 25 papers in conferences and has been involved many international conferences as Technical Chair and tutorial presenter. He is an active member of IEEE, ISTE, IAENG, IACSIT and Indian Computer Society.