Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Data Verification Process by Homomorphism Encryption in Cloud

Yogesh Vishwakarma, Prof. Vineet Richariya
Computer Science & RGPV University
Madhya Pradesh, India

Abstract—Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing, untrusted cloud servers, and the data access control becomes a challenging issue in cloud storage systems. Cloud Computing has been the most promising innovation in the computing world in past decade. Its usage is still blocked by the security concerns related with critical data. The encryption of remotely laid in data has been the most widely used technique to bridge this security gap. The speculated vast usage of Cloud Computing solutions for data storage and with Big Data Analytics gaining strong foothold; the security on cloud is still at big risk. Fully Homomorphic Encryption is a good basis to enhance the security measures of un-trusted systems or applications that stores and manipulates sensitive data. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis is assumed to show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Keywords— Homomorpic Encryption, Cloud Computing, security in cloud computing, cloud security, Homormorpic in cloud computing

I. INTRODUCTION

Cloud computing is a recent technological development in the computing field in which mainly focused on designing of services which can be provided to the users in same way as the basic utilities like food, water, gas, electricity and telephony. In this technology services are developed and hosted on the cloud (a network designed for storing data called data enter) and then these services are offered to users always whenever they want to use. The cloud hosted services are delivered to users in pay-per-use, multi-tenancy, scalability, self-operability, on-demand and cost effective manner. Cloud computing is become popular because of above mention services offered to users. All the services offered by servers to users are provided by cloud service provider (CSP) which is working same as the ISP (Internet service provider) in the internet computing. In the internet technology some innovative development in virtualization and distributed computing and accessing of high speed network with low cost attract focus of users toward this technology. This technology is designed with the new concept of services provisioning to users without purchasing of these services and stored on their local memory.

Architecture

In the cloud computing architecture of service provisioning, basically three parties are involved for providing services to the users:-

1. User/Client
2. Third Party Auditor (TPA)
3. Cloud Server (CS)

User/Client

In the cloud computing architecture, user is the one who uses the services of cloud. It may be a mobile device or stationary device which request for services to the cloud service provider and then on the basis of user's requests Third Party Auditor (TPA), provides demanded services to these users offered by the Cloud Server (CS). In the cloud computing data is stored in data centres from where data is accessed when or wherever it is required. With the data centres virtual servers are connected in which one or more virtual machines (VM) are situated for computation.

Third Party Auditor (TPA)

Third Party Auditor (TPA) is the third party between cloud user and cloud service providers which is responsible for secure service provisioning. In the figure 1 we can see that how third party auditor providing services between users and cloud servers securely. TPA performs some operation for agreement and verification between users and service provider for security purpose.

Cloud Service Provider (CSP)

Cloud service provider offered private, public and hybrid cloud networks with strong service-level agreement, better customer satisfaction and cost effective manner. CSP offers services to the users in such a way so that if it is required to configure a service than user has the opportunity to configure the available services according to their uses and security premises.

Cloud Service Models

The services provided by the cloud computing are divided into three universally accepted categories these are Infrastructure-as-a-Service [2] (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Basically these three service models are interrelated to each other and designed 3-tiers architecture. Figure 2 shows 3-tier architecture of cloud computing.

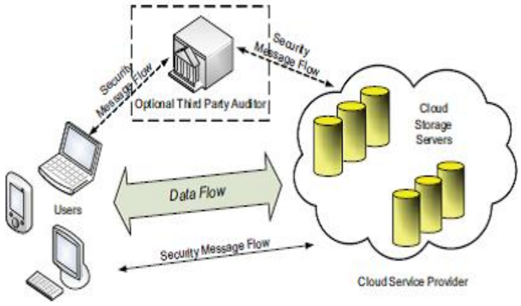


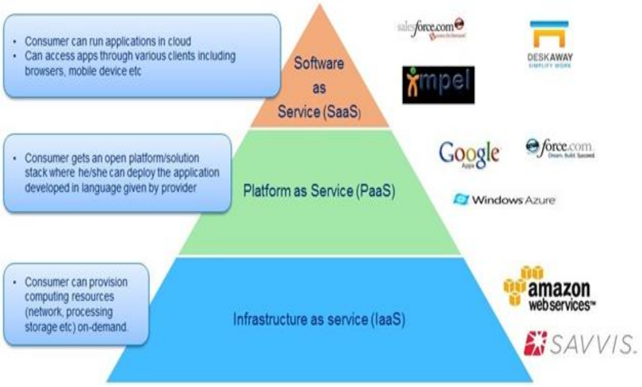
Figure 1.1 Cloud computing TPA service provisioning architecture

Platform-as-a-Service (PaaS):-

This is second or middle layer of 3-tier architecture. In this model a platform is provided to users which typically include operating system, programming languages, execution environments, databases, queues and web servers. Examples are AWS Elastic Beanstalk, Heroku, Force.com and Google App Engine. Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider's infrastructure. Developers make application on the provider's platform over the Internet. Platform as service providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com and GoogleApps are illustretaion of PaaS. Developers need to know that currently, there are not criteria for interoperability or data portability in the cloud. Some providers will not always allow software created by their customers to be moved off the provider's platform.

Software-as-a-Service (SaaS):-

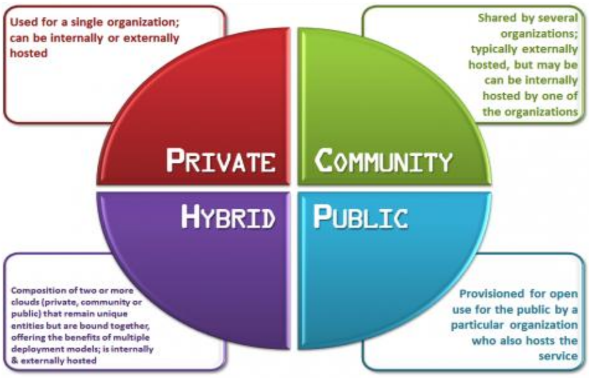
This is third or upper layer of 3-tier architecture. This model provides “On-demand software’s” to users without installation setup and running of the applications. Users have to pay and use it through some client. Examples are Google Apps and Microsoft office 365. In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product & interacts with the user through a front-end portal. Software as a service is a very broad market. Services can be anything from Web-based email to inventory control and database processing. It’s the service provider hosts both the application & the data, the end user is free to use the service from anywhere.


Consumer can run applications in cloud
Can access apps through various clients including browsers, mobile device etc
Software as Service (SaaS)
salesforce.com
DESKAWAY
impel
Consumer gets an open platform/solution stack where he/she can deploy the application developed in language given by provider
Platform as Service (PaaS)
Google Apps
force.com
Windows Azure
Consumer can provision computing resources (network, processing storage etc) on-demand
Infrastructure as service (IaaS)
amazon web services
SAVVIS.

Cloud service modal

Cloud Types

There are four types of clouds [4]:- private cloud, public cloud, community cloud & hybrid cloud from the physical location of user’s point of view.


Used for a single organization; can be internally or externally hosted
Shared by several organizations; typically externally hosted, but may be can be internally hosted by one of the organizations
PRIVATE
COMMUNITY
HYBRID
PUBLIC
Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted
Provisioned for open use for the public by a particular organization who also hosts the service

Types of cloud

Private cloud:-

A private cloud is one which is setup by single organization and installed services on its own data center. A private cloud is a proprietary network or a data centre that supplies hosted services to a limited number of persons. When a service provider uses public cloud resources to create their private cloud, then the result is called a virtual private cloud.

Public cloud:-

A Public cloud services are offered by third-party cloud service providers and involve resource provisioning outside of the user's premises. A public cloud sells services to anyone on the Internet. Currently, Amazon Web Services is the huge public cloud provider.

Community cloud:-

The Community [18] cloud can offer services to the cluster of organizations.

Hybrid cloud:-

A Hybrid cloud is the combination of any two or more types of above mentioned cloud types.

A cloud can be of any type but the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

II. LITERATURE REVIEW

Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang-Feb 2013, IEEE

Proposed a work TPA to perform audits for multiple users simultaneously and efficiently they performed batch auditing support where multiple file can be audit without knowledge of data to the tpa and cloud. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. They have enables an external auditor to audit user's cloud data without learning the data content, multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner, MAC based setup has been performed and hashing algorithm is used to perform auditing while dealing with the data. HLA and MAC based technique has been used to perform the experimentally setup and performed the results. the results and performance analysis has been done in various aspects such as they have taken some sample blocks and computes the various result parameters server computation time and cloud computation time and communication cost. the holomorphic linear authenticator and random masking is used in this scheme to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

Rachna Arora, Anshu Parashar, June-2013,

Secure User Data in Cloud Computing Using Encryption Algorithms proposed a scheme for cloud security they proposed different security algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing web application on cloud. Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption/decryption of messages whereas DES (Data Encryption Standard) was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES (Advanced Encryption Standard) was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128, 192, 256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits.so in this paper the authors have performed various algorithms and compared the results out of all the algorithms.

Characteristics	**AES**	**RSA**	**BLOWFISH**	**DES**
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Key Size	128,192,256 bits	1024 bits	32-448 bits	56 bits
Key Used	Same key is used to encrypt and decrypt the blocks.	Public key is used for encryption and private key, for decryption	Same key is used for both encryption and decryption of data.	For encryption and decryption same key is used.
Scalability	Scalable	Not Scalable	Scalable	Scalable
Initial Vector Size	128 bits	1024 bits	64 bits	64 bits
Security	Secure for both provider and user.	Secure for user only	Secure for both providers and user/client side	Security applied to both providers and user

Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo "An Efficient Signature Scheme from Bilinear Pairings and Its Applications"

Propose a new short signature scheme from the bilinear pairings that unlike BLS, uses general cryptographic hash functions such as SHA-1 or MD5, and does not require special hash functions. Furthermore, the scheme requires less pairing operations than BLS scheme and so is more efficient than BLS scheme. this signature scheme to construct a ring signature scheme and a new method for delegation. We give the exact security proofs for the new signature scheme and the ring signature scheme in the random oracle model. a new short signature scheme that is more efficient than BLS scheme. The security of this signature scheme depends on a new problem, namely k-CAA or k + 1EP. It is shown that k + 1EP is no harder than the CDHP. Based on this basic signature scheme, a ring signature scheme and a new method for delegation are proposed in this paper research, bilinear algorithm is a pairing based algorithm which is privacy preserving and able to perform the data security without interruption and hiding the original data without interruption in the auditing process and the hashing was performed with the help of sha-1 which produce 128 bit key length in order to maintain the data in checksum process in verification, they have used JPBC java library in order to perform the execution and perform the simulation for the present algorithm , the Boneh-Lynn-Shacham signature scheme allows a user to verify that a signer is authentic. The scheme uses a pairing function for verification and signatures are group elements in some elliptic curve. Working in an elliptic curve provides defense against index calculus attacks against allowing shorter signatures than FDH signatures. Signatures are often referred to as short signatures, BLS short signatures, or simply BLS signatures. The signature scheme is provably secure (that is, the scheme is existentially unforgeable under adaptive chosen-message attacks) assuming both the existence of random oracles and the intractability of the computational Diffie-Hellman problem.

Zhifeng Xiao and Yang Xiao,IEEE June 2013 conference – "Security and Privacy in Cloud Computing"

They have worked on various attribute confidentiality, integrity, availability, accountability, and privacy-preservability and performed the various security concern issues in aspects, authors have systematically studied the security and privacy issues in cloud computing based on an attribute-driven methodology, We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability and privacy-preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well, thus this is the paper included the security and study aspects in cloud computing, the data integrity verification made dealing with encryption algorithm and the audit was performed with the help of hashing algorithm available in order to verify the value generated again while checking the data integrity available with the associated file, here they have worked on different aspects such as user account access approach, availability of data, data changing or integrity verification and the technique should be privacy preserving so that the data should not be leak during the cloud execution.

Hovav Shacham, Brent Waters stated "compact proof of retrievability"

the cloud must provide the proof that its providing or maintaining complete data storage and in that they have stated to provide the proof that is data is maintaining by the cloud, there they have stated the file information related to computer MAC address related to which data was generated and they have used MAC as a data integrity proof, their system allow for compact proofs with just one authenticator value this can lead to proofs with as little as 40 bytes of communication. They have provided two solutions for it two solutions with similar structure. The one is privately veriable and builds elegantly on pseudorandom functions (PRFs); the second allows for publicly veriable proofs and is built from the signature scheme of Boneh, Lynn, and Shacham in bilinear groups. Both solutions rely on homomorphism properties to aggregate a proof into one small authenticator value. They have worked with the parameters such as efficiency, public verifiable, public retrievable – where efficiency they have stated that the system should be as efficient as possible in terms of both computational complexity and communication complexity, that was given an emphasis to work on and A system is publicly verifiable if any (untrusted) entity can perform the verification audit. This is desirable in settings where many users might shareable storage or when a third party is employed to audit the storage servers.in the paper they have specified two schemes redundantly encode able with an erasure code and apply an audit that probabilistically ensures enough blocks are retrievable to reconstruct the file.

Different Encryption Technique Results:

Encryption Algorithm	**Key Length**	**Computation time(in ms)**
AES	2048	2390
Blowfish	1024	500
RC4	1024	169
RSA-1,2	1024,2048	5199
KB-ABE	2048	346

Different Hashing Technique Result:

Hashing Algorithm	**Key Length**	**Rounds**
MD5	128	48
SHA-1	160	80
SHA-2	224	64
SHA-3	256	24

III. EXISTING SYSTEM

The traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes cannot work on the outsourced data. it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, it is crucial to realize public audit ability for CSS, so that data owners may resort to a third party auditor, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds. To implement public audit ability, the notions of proof of irretrievability and provable data possession have been proposed by some researchers. Their approach was based on a probabilistic proof technique for a storage provider to prove that clients' data remain intact.

IV. DISADVANTAGES

1) Lack of rigorous performance analysis for constructed audit system greatly affects the practical application of this scheme.
2) it is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which possible adversary's advantage through dynamic data operations should be prohibited
3) Single TPA to audit for all files and to take more time to auditing the files.

V. PROPOSED SYSTEM

In the proposed work on monitoring other technique we are presenting some modules in which we will encrypt the data and further outperform the auditing technique which is hash based technique for data integrity verification. Furthermore, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services in homomorphic encryption algorithm using SHA-2 hashing technique. A proof of- concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show our system has a lower computation cost, as well as a shorter extra storage for integrity verification.

VI. PROPOSED SYSTEM

1. A fragment technique is introduced in this paper to improve performance and reduce extra storage.
2. The audit activities are efficiently scheduled in an audit period, and a TPA needs merely access file to perform audit in each activity.
3. Each TPA to audit for a batch of files and to save the times for auditing the files.

VII. MODULE

1. Key Generation:

The owner generates a public/secret key pair (pk, sk) by himself or the system manager, and then sends his public key pk to TPA. Note that TPA cannot obtain the client's secret key sk; secondly, the owner chooses the random secret.

2. Tag Generation:

The client (data owner) uses the secret key SK to pre-process a file, which consists of a collection of n blocks, generates a set of public verification parameters and index-hash table that are stored in TPA, and transmits the file and some verification tags to CSP.

3. Periodic Sampling Batch Audit:

The Batch TPA (or other applications) issues a "Random Sampling" challenge to audit the integrity and availability of outsourced data in terms of the verification information stored in TPA.

4. Audit for Dynamic Operations:

An authorized application, which holds data owner's secret key sk, can manipulate the outsourced data and update the associated index hash table stored in TPA. The privacy of sk and the checking algorithm ensure that the storage server cannot cheat the authorized applications and forge the valid audit records.

VIII. CONCLUSIONS

Our discussion involve in the field of cloud security such as encryption technique to store data and unauthorized access to the data. Also our work in this paper discuss about the technique been performed in the cloud. The motivation for the work is to find a best technique which take a less time but high security to the encrypted data store in cloud. Our further work will concentrate on finding an encryption technique and auditing technique which perform well while verifying the data integrity.

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] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011.

[3] C. Wang, B. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from theWeil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), pp. 514-532.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[6] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[7] M. 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," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010.

[9] Rachna Arora*, Anshu Parashar," Secure User Data in Cloud Computing Using Encryption Algorithms",IJERA Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[10] Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo "An Efficient Signature Scheme from Bilinear Pairings and Its Applications".

[11] Dimitrios Zissis , Dimitrios Lekkas in Elsevier –" Addressing cloud computing security issues- Future Generation Computer Systems 28 (2012) 583–592.

[12] Boyang Wang, Baochun Li in IEEE transaction "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud",2014.