Enhancing Data Integrity Proofs with Cloud Storage Security

Pooja Patel

Silver Oak College of Engineering and Technology, Gujarat Technological University, S. G. Highway, Gota, Ahmedabad, India

Abstract: ***Cloud computing is fast growing technology which facilitates more and more users and organizations shifting towards opting their services to cloud. Data security is considered as the constant issue leading towards a hitch in the adoption of cloud computing. Due to large spread of the information through last few years there is a massive need of securing the contents from threats. With the help of cloud computing now we are able to transfer the data and share the information very easily from one place to another with in no time. But the whole process is done on net, on internet so the basic need of that transferring data and storage data are to be secure. The prime objective is to give effective and efficient method for cloud storage security in cloud computing. We are analyzed types of cloud storage and security aspects in cloud.***

Keywords: cloud computing; cloud storage; data integrity; data Confidentiality; data availability; data privacy; data trust; data location

1. Introduction

Cloud computing is in its infant form and numerous definitions have been proposed by many scientists. The National Institute of Standards and Technology defines cloud computing as “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, (for example networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”[1]. The word “cloud” has been popular by the marketers, which refers to a service such as the applications or the infrastructure or the platform that underlies cloud computing technology beneath them. Cloud computing provides the user ability to store their data and execute processes on a virtualized environment, and also an ease of utilization of the physical resources. Despite the advantages that cloud computing offers, there are many challenges and the biggest being security risks that overshadow the growth of cloud computing infrastructure.

Cloud computing ,which is the use of computing resources that are delivered as a service over a network like the internet on pay-as-usability basis, is composed of three main service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[2]. In Infrastructure-as-a-Service (IaaS), isolation should consider VM’s storage, processing, memory, cache memories, and networks. In Platform-as-a-Service (PaaS), isolation should cover isolation among running services and API’s calls. In Software-as-a-Service (SaaS), isolation should isolate among transactions carried out on the same instance by different tenants and tenant’s data [13].

Cloud computing provides five essential characteristics which are:

- **Resource Pooling**: In this resources are pooled to serve multiple users’ using a multi tenant model, with different virtual and physical resources dynamically assigned and reassigned according to consumer demand. In this location is independent that is the customer has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., datacenter, state or country).
- **Broad network access**: In this capabilities are available over the network and accessed through standard mechanism.
- **On demand self-service**: A consumer can provision server time as network storage, as needed automatically without requiring human interaction with each service’s provider.
- **Measured Service**: Cloud systems control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., bandwidth, storage and processing). Resource usage can be controlled, monitored and reported providing transparency for both the consumer and provider of the utilized service.
- **Rapid elasticity**: Capabilities can be elastically and rapidly provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

2. Cloud Storage

While cloud storage is convenient and gives employees access to their data anywhere, at any time, on nearly any device, cloud storage security is a top concern for organizations’ IT and security departments. The benefits brought by cloud storage – from scalability and accessibility to decreased IT overhead – are driving rapid adoption at enterprises around the world, and there are steps that companies should take to improve cloud storage security and keep sensitive data safe and secure in the cloud.

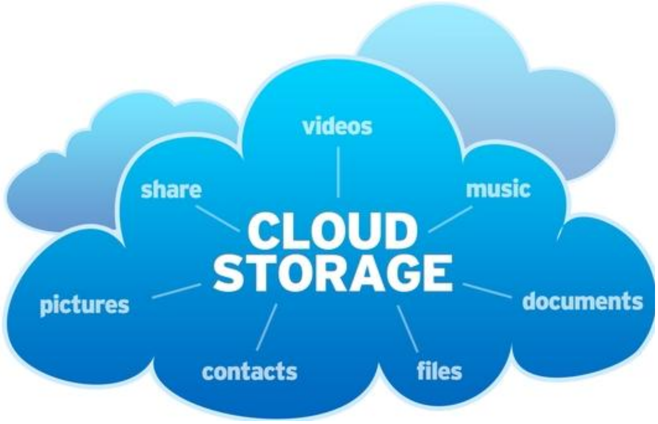

Figure 1: Cloud Storage

There are four main types of cloud storage:

- Mobile Cloud Storage: it stores the individual's data in the cloud and provides access to the data from anywhere [2].
- Public Cloud Storage: There is no connection between the enterprise and storage service provider. Management of resources is fully audited in the cloud storage provider's environment [2].
- Private Cloud Storage: the infrastructure exists in the enterprise's data center that is typically managed by the storage provider and only the enterprise has access to it [2].
- Hybrid Cloud Storage: it is a combination of public and private cloud storage where crucial data resides in the enterprise's private cloud whereas other data is stored in a public cloud storage provider [2].

2.1 Need for Cloud Storage Security

Businesses and enterprises use cloud services because they provide cost-effective and flexible alternatives to expensive, locally-implemented hardware. But conducting business in the cloud means that confidential files and sensitive data are exposed to new risks, as cloud-stored data resides outside of the limits of many safeguards used to protect sensitive data held on-premise. As such, enterprises must take additional measures to secure cloud storage beyond the sometimes basic protections offered by providers.

3. Security Aspects

These properties have become the key aspects used in designing secure systems, especially, in the case of cloud computing architecture.

3.1 Data Confidentiality

It refers only to authorized parties or systems having the ability to access protected data [4]. Outsourcing data, delegating its control to a cloud provider and making it accessible to different parties increase the risk of data breach. A number of concerns emerge regarding the issues of multi-tenancy, application security and privacy [5]. Multi-tenancy refers to the cloud characteristic of resource sharing [4]. The cloud computing architecture consists of sharing different kinds of resources to enable multiple clients to use the same resource at the same time which presents a number of privacy and confidentiality threats.

3.2 Data Integrity

It means that only authorized parties can modify assets in authorized ways and it refers to data, software and hardware. Data Integrity refers to protecting data from unauthorized deletion, modification or fabrication [4]. Authorization is the mechanism used by the system to determine what level of access a particular authenticated user should have to secure resources [4]. Due to the rise of the number of parties involved in a cloud environment, authorization is important to ensure data integrity.

3.3 Data Availability

It refers to the property of a system being accessible and usable upon demand by an authorized entity. System availability includes a system's ability to carry on operations even when some authorities misbehave [4]. To ensure availability, the system has to be able to operate even if there is a security threat. The user of a cloud environment, who is discharged of hardware infrastructure requirements, relies on the availability of the ubiquitous network.

3.4 Data Privacy

The privacy threats faced by cloud computing are the complexity associated with the risk assessment, growing industry demands the emergence of timely delivery of new business models and its implications on consumer privacy , various regulatory compliance, data privacy issues in design leading towards poor data quality and also lack of transparency [6].

3.5 Data Trust

Trust is the major concern is and it breaks if two issues are not handled properly one of them is lack of transparency and other is due to breach in security and privacy. The cloud service providers offer flexibility to the use of resources which attracts consumers of cloud computing to get benefitted from the service by involving their sensitive data at risk [3]. Trust is based on the security which the cloud service provider gives to its customers. Furthermore, trust mechanisms need to be propagated right along the chain of service provision [11].

3.6 Data Location

Location of end-user data is of great importance. Cloud users whose information assets require location-specific data storage or transit requirements must confirm these with cloud providers that offer location-based cloud service, and must ensure that they are included in the service contract offered by the cloud provider [12].

4. Literature Review

Data security is considered as the constant issue leading towards a hitch in the adoption of cloud computing. Data privacy, Integrity and trust issues are few severe security concerns leading to wide adoption of cloud computing [3].

Many different techniques have been proposed to solve the problems of security in cloud computing.

In paper [3] the author proposes an approach for Cloud Computing Data Storage Security relating to Data Integrity, Privacy and Trust. The proposed data security model uses a three layer system structure in which these layers are used for ensuring data security. In this model, all the techniques and mechanism useful for implementing a highly protected environment is developed. The end user will access the cloud through internet and for that strong log in access is provided to the user. The high security login feature in the model will prevent the user with malicious intent to use the data stored on the cloud. The software encrypts and protects data at various levels by using various security techniques and security algorithms. The first-layer: This layer is responsible for the authentication of the user; in this layer the cloud service provider can use their authentication methods for ensuring the genuine user. The Second layer: This layer communicates with the previous layer to make sure that only authorized user can send receive the data. This layer has cryptographically enforced Data Centric Security. The Third layer: This layer is responsible interacting with the second layer and ensures that user requested the data for processing from storage is genuine.

In paper [7] the author talked about a scheme which does not involve the encryption of the whole data. They encrypt only few bits of data per data block thus reducing the computational overhead on the clients. The client storage overhead is also minimized as it does not store any data with it. Hence their scheme suits well for thin clients. In their data integrity protocol the verifier needs to store only a single cryptographic key - irrespective of the size of the data file F- and two functions which generate a random sequence. The verifier does not store any data with it.

In paper [8] used HMAC and SHA-256 technique for verify the integrity of information passed between applications. In this work consists of four algorithms: KeyGen, SigGen, GenProof, and VerifyPoof. KeyGen is run by the cloud user to setup the scheme. SigGen is used by the cloud user to generate verification metadata, which may consist of MACs, signatures, or other related information that will be used for auditing. The SigGen is used to generate the file tags, by applyingHMAC-SHA-256(Enc (data)). GenProof is run by the cloud server to generate a proof of data storage correctness. VerifyProof is run by the TPA to verify the proof received from the cloud server.

In paper [2] presents mobile cloud middleware storage for mobile clients which provides a lightweight data security mechanism with respect to limited resources of mobile devices and wireless in mobile computing environments. In addition, to unlimited storage area for the mobile client files and data. A middleware enhance interaction between mobile devices and cloud services. Generally, the middleware improves the functionality, and reliability of the interaction between mobile clients and cloud services [9]. The system, will contribute to provide the mobile client with a reliable and unlimited storage, along with a secured data access in addition to an efficient data retrieving which are the prime objectives when designing our middleware. Currently, the System is in the prototype stage.

In paper [10] the author propose a novel AUDITING scheme with public verification based on self certified signature in the paper to overcome low efficiency problem and attack problem. The scheme can efficiently resist data leakage and active attack. The scheme has constant communication cost and public verification in the data integrity checking. The scheme reduces the computation cost of producing data authentication tag before the outsourcing data. The security of this scheme is based on the fixed inversion problem (FI) of the bilinear map and the inversion of hash function. In this system model consists of four entities: the trust authority, data owner, the verifier and the cloud. The trust authority is responsible to issue key for data user. Data owner has a number of data and stores them on the cloud server after erasure coding together with the corresponding signatures on these data. The verifier is able to execute the integrity checking of the outsourced data on behalf of the data owner. To execute the integrity checking of data, the verifier needs to produce a challenging message and sends it to the cloud server. The cloud server needs to respond the computed proof for the selected file blocks to the verifier besides managing and storing these outsourced data of data owner.

5. Conclusion

The adoption of cloud computing paradigm is continuously growing. Concerning about security is an important factor that affect the popularity of cloud computing. Cloud storage is more and more attractive because it can realize the sharing and storing of data files among companies and corporations. Data storage correctness is one of these challenges, when the users store their data remotely in the cloud. However, for the data owner, the most concern is the integrity of data file. We identified the key challenges and research dimensions that need to be addressed in the data integrity in cloud storage security. Finally, we provided a comprehensive analysis of the technical attributes of cloud storage security; an insight to technology, services, strategies & practices currently followed in this field and a survey of existing security frameworks & identifications of future directions that are expected to drive innovation in this cloud computing domain.

References

[1] Sana Belguith, Abderrazak Jemai, Rabah Attia, “Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm”, *ICAS 2015*

[2] Khadija Akherfi, Hamid Harroud and Michael Gerndt , “A Mobile Cloud Middleware for Data Storage and Integrity”, 978-1-4673-8149-9/15/$31.00 ©2015 IEEE

[3] Preeti Sirohi and Amit Agarwal, “Cloud Computing data Storage Security framework relating to data Integrity, Privacy and Trust”,978-1-4673-6809-4/15/$31.00 ©2015 IEEE

[4] D. Zissis and D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems, 28(3), 2012, pp. 583-592

[5] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010

[6] D. Chen, Data security and Privacy Protection issues in Cloud Computing, Computer Science and Electronics Engineering (ICCSEE)International Conference, 2012, PP 647-651

[7] Sravan Kumar R and Ashutosh Saxena ,"Data Integrity Proofs in Cloud Storage", 978-1-4244-8953-4/11/$26.00 c 2011 IEEE

[8] Salah H. Abbdal, Hai Jin, Deqing Zou, Ali. A. Yassen , "Secure third Party Auditor for Ensuring Data Integrity in Cloud Storage" 978-1-4799-7646-1/14 $31.00 © 2014 IEEE

[9] S. Ilarri, E. Mena, and A. Illarramendi, "A system based on mobile agents to test mobile computing applications," Journal of Network and Computer Applications, vol. 32, no. 4, pp. 846-865, Jul, 2009.

[10] Jianhong Zhang, Weina Zeng, "Self-certified Public Auditing for Data Integrity in Cloud Storage", 978-1-4799-4171-1/14 $31.00 © 2014 IEEE

[11] S. Pearson and A. Benameur, Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science, Cloudcom-2010.66, PP 693-702

[12] C. Onwubiko, N. Antonopoulos and L. Gillam, Security Issues to cloud computing, DOI 10.1007/978-1-84996-241-4_16,Springer-Verlag London Limited 2010

[13] Huaglory Tianfield, Security Issues In Cloud Computing, IEEE international Conference on Systems, Man, and Cybernetics, COEX, Seoul, Korea, 978-1-4673-1714-6/12/$31.00 © 2012 IEEE

Author Profile

Mrs. Pooja Patel received her B.E. degree from L.D College of Engineering, under Gujarat Technological University in 2015. She is currently pursuing her M.E. at Silver Oak College of Engineering and Technology, under Gujarat Technological University. Her research interests include Cloud computing security.