Security in Cloud Computing- Hash Function

Paridhi Singhal
(Department of Computer Science
&
Engineering), FET
MITS Lakshmangarh, Rajasthan,
India

Alok Garg
Test Lead
CanvasM Technologies Limited
(A Tech Mahindra Subsidiary)
Noida, India

Manoj Diwakar
(Department of Computer Science
&
Engineering), DIT Dehradun,
Uttarakhand, India

ABSTRACT

There is a critical need to securely store, manage, share and analyze massive amounts of complex (e.g., semi-structure and unstructured) data to determine patterns and trends in order to improve the quality of healthcare, better safeguard the nation and explore alternative energy. Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore we need to safeguard the data in the midst of entrusted processes. In this method some important security services including authentication, encryption and decryption are provided in Cloud Computing system.

Keywords

Security, Credentials, Data Encryption, Authentication, Hash Function.

1. INTRODUCTION

Cloud computing providers offer their services according to three fundamental models [1]: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models figure1. In 2012 network as a service (NaaS) and communication as a service (CaaS) were officially included by ITU (International Telecommunication Union) as part of the basic cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem. The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries now a days. Since the security is not provided in cloud, many companies adopt their unique security structure [2]. For e.g. Amazon has its own security structure.

Storing data and using other software-as-a-service or cloud computing models to solve contemporary business and personal data storage problems has been viewed as unusual and often impractical. However, in today's world, when Internet speeds are so fast that a single document maybe uploaded in seconds, cloud computing makes a lot more sense. The fact is, a laptop or hard drive can be lost, damaged, or stolen, but the cloud cannot if you are choosing a software service provider who uses multiple backup systems. Another advantage of online storing [3] your data in the cloud is access. If you work with a cloud company, you can download your documents, photos, or other data from any computer or laptop anywhere in the world. Cloud storage has significant security implications. Using an encrypted and secured server to store your confidential data securely will make it easier to ensure that you or your clients' information is safe. If you store data on your private computer and it is stolen, eventually a criminal may be able to break the password and steal the data. If you store your data in the cloud, the password and username you use to access the data can be changed and reset immediately. It is important to save to the cloud not only finished documents, but also working drafts, to ensure that your data protection is consistent.

Cloud technology has other values besides data storage. There are many companies that offer cloud sourcing of document creation to ensure that tasks are completed as quickly and cheaply as possible. Many of these workforce-as-a-service companies take advantage of workers with expertise in your subject matter who live all over the world and may not be available for more traditional employment.

Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle in this paper. Since the data placed in the cloud is accessible to everyone, security is not guaranteed .I propose a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.

As cloud computing has taken hold, there are many major benefits that have become clear:

1. Reduced IT costs: Moving to cloud computing may reduce the cost of managing and maintain your IT systems. Rather than purchasing expensive systems and equipment for your business, you can reduce your costs by using the resources of your cloud computing service provider. You may be able to reduce your operating costs because:
   - The cost of system upgrades, new hardware and software may be included in your contact.
   - You no longer need to pay wages for expert staff.
   - Your energy consumption costs may be reduced.
   - There are fewer time delays.
2. Scalability: Your business can scale up or scale down your operation and storage needs quickly to suit your situation, allowing flexibility as your needs change. Rather than purchasing and installing expensive upgrades yourself, your cloud computing service provider can handle this for you.

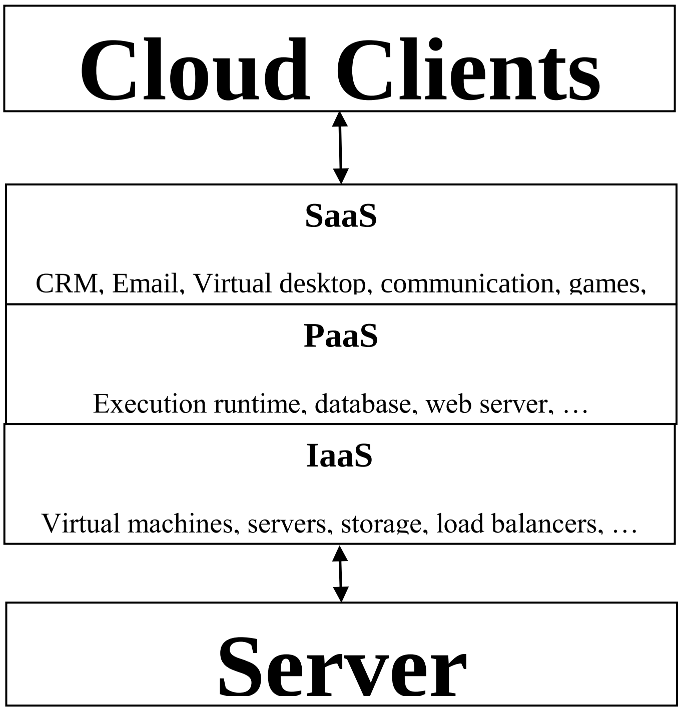
Cloud Clients
SaaS
CRM, Email, Virtual desktop, communication, games,
PaaS
Execution runtime, database, web server, …
IaaS
Virtual machines, servers, storage, load balancers, …
Server

Figure1. Cloud infrastructure

Using the cloud frees up your time so you can get on with running your business.

3. Business Continuity: Protecting your data and systems is an important part of business continuity planning. Whether you experience a nature disaster, power failure or other crisis, having your data storage in the cloud ensures it is backed up and protected in a secure [4] and safe location. Being able to access your data again quickly allows you to conduct business as usual, minimizing any downtime and loss of productivity.
4. Collaboration Efficiency: Collaboration in a cloud environment gives your business the ability to communicate and share more easily outside of the traditional methods. If you are working on a project across different locations, you could use cloud computing to give employees, contractors and third parties access to the same files. You could also choose a cloud computing model that makes it easy for you to share your records with your advisers.
5. Flexibility of work practices: Cloud computing allows employees to be more flexible in their work practices. For example, you have the ability to access data from home, on holiday, or via the commute to and from work. If you need access to your data while you are off-site, you can connect to your data while you are off-site, you can connect to your virtual office, quickly and easily.
6. Access to automatic updates: Access to automatic updates for your IT requirements may be included in your service fee. Depending on your cloud computing service provider, your system will regularly be updated with the latest technology. This cloud includes up-to-date versions of software, as well as upgrades to servers and computer processing power.

2. EARLY WORK

2.1 Toward Publicly Auditable Secure Cloud Data Storage Services

The authors propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. The author describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality [5].

2.2 Identity-Based Authentication for Cloud Computing

The authors propose an identity-based encryption (IBE) and decryption and identity-based signature (IBS) schemes for IBHMCC. Based on the former IBE and IBS schemes, an identity based authentication for cloud computing (IBACC) is proposed. The author presented an identity based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes [6]. The authors proposed Identity-based Authentication Protocol. Identity-based Authentication Protocol contains sequence of steps. In step (1), the client C sends the server S a Client Hello message. The message contains a fresh random number C n, session identifier ID and C specification. In step (2), the server S responds with a Server Hello message which contains a new fresh random number S n, the session identifier ID and the cipher specification S specification the cipher text is transmitted to C as Server Key Exchange message. Then S generates a signature Sig S S [M] as the Identity Verify message to forward to C. Finally, The Server Hello Done message means the step (2) is over. In step (3), C firstly verifies the signature S Sig S S with the help of
S ID Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight than SAP, especially the more lightweight user side.

2.3 Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance [7]. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users [8]. Figure2[9]: The architecture of cloud data storage service The Cloud Computing model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called Cloud servers, and service requesters, called clients. Often clients and servers.

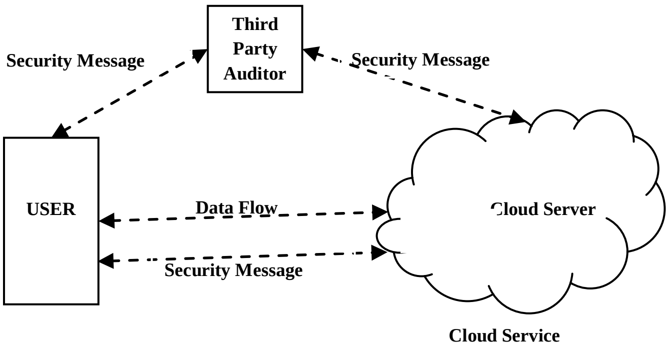

Figure 2: The architecture of cloud data storage service

3. EXISTING SYSTEM

Introducing an effective third party auditor (TPA) for privacy and security, the following fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. This scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The security and performance is justified through concrete experiments and comparisons with the state-of-art. In cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful employment of the cloud architecture. Another problem is that data stored in the cloud does not remain static [10].

4. PROPOSED SYSTEM

The Proposed Network consists of three backup sites for recovery after disaster. The backup sites are located at remote location from the main server. If any one of the paths fails it uses alternate path working [9]. The encrypted file will be creating during back up sites. The data will be decrypted during recovery operation. Proposed a cross platform integration model using secure communication via the Internet and the utilization of a key for security.

Client sends the data to the server which is known as Main Server. At the same time data is also back up to Multi Servers. In this method for data backup it involve with three Multi Server such as (SA 1(Server, Application), SA 2, SA 3, etc…). Multi-server sends the key id to our mail id. The data is to be encrypted figure3 in multi-server. In encryption the data that has to stored in a cloud cannot be stored in a text format due to security reasons so it must be transformed into an encrypted format. This method deals with the encrypts the data before it is taken as back up in multi server. To encrypt the data’s Hash Function is used. Suppose the data is deleted in the client system. Then we authenticate the data through following procedures: Find the key in our email id. Give the file name and date in login form.

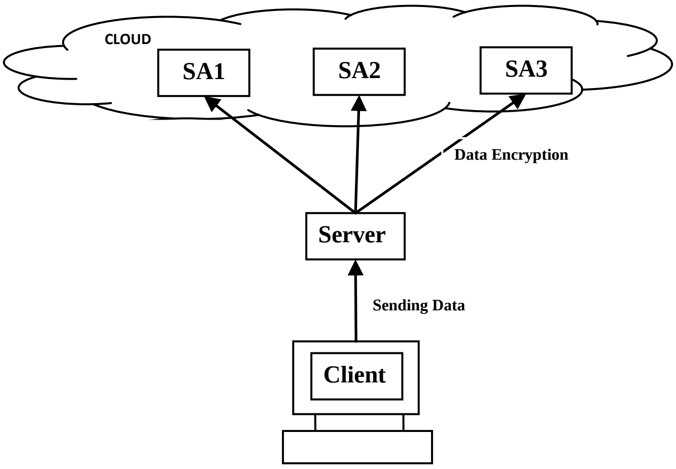

Figure3: Data Backup

5. HASH FUNCTION

A variation on the message authentication code is the one-way hash function. As with the message authentication code, a hash function accepts a variable-size message M as input and produces a fixed-size output, referred to as a hash code H (M). The hash code is aloes referred to as a Message Digest or Hash Value. The hash code is a function of all the bits of the message and provides an error-detection capability: A change to any bits in the message

Table1: Basic Uses of Hash Function H

<table>
<tr><td>A→B: E(K,[M||H(M)])
(a) Encrypt message plus hash code</td><td>A→B: E(K,[M||E(PR_a, H(M))])
(d) Encrypt result of (c)-shared secret key</td></tr>
<tr><td>A→B: M||E(K,H(M))
(b) Encrypt hash code-shared secret key</td><td>A→B: M||H(M||S)
(e) Compute hash code of message plus secret value</td></tr>
<tr><td>A→B: M||E(PR_a, H(M))
(c) Encrypt hash code-sender's private key</td><td>A→B: E(K,[M||H(M||S)])
(f) Encrypt result of (e)</td></tr>
</table>

results in a change to the hash code. There are many ways in which a hash code can be used to provide message authentication, as follows:

a) The message plus concatenation hash code is encrypted using symmetric encryption. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, confidentiality is also provided.
b) Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality. Note that the combination of hashing and encryption results in an overall function. That is, E (K, H (M)) is a function of a variable-length message M and a secret key K, and it produces a fixed-size output that is secure against an opponent who does not know the secret key.
c) Only the hash code is encrypted, using public key encryption and using the sender's private key. As with (b), this provides authentication. It also provides a digital signature, because only the sender could have produces the encrypted hash code. In fact, this is the essence of the digital signature technique.
d) If confidentiality as well as digital signature is desired, then the message plus the private-key-encrypted hash code can be encrypted using a symmetric secret key. This is a common technique.
e) It is possible to use a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. a computes the hash value over the concatenation of M and S and appends the resulting hash value to M. because B possesses S, it can recomputed the hash value to verify. Because the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.
f) Confidentiality can be added to the approach of (e) by encrypting the entire message plus the hash code.

When confidentiality is not required, methods (b) and (c) have an advantage over those that encrypt the entire message in that less computation is required Table1.

Nevertheless, there has been growing interest in technique that avoids encryption. Several reasons for this interest are pointed out in [11]:

1. Encryption software is relatively slow. Even though the amount of data to be encrypted per message is small, there may be a stream of messages into and out of a system.
2. Encryption hardware costs are not negligible. Low-cost chip implementations of DES are available, but the cost adds up if all nodes in a network must have this capability.
3. Encryption hardware is optimized toward large data sizes. For small blocks of data, a high proportion of the time is spent in initialization/invocation overhead.
4. Encryption algorithms may be covered by patents. For example, until the patent expired, RSA was patented and had to be licensed, adding a cost.

6. CONCLUSION

Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users [12]. Responsible management of personal data is a central part of creating the trust that underpins adoption of cloud based services – without trust, customers will be reluctant to use cloud-based services [13]. Authentication is necessary in Cloud Computing. After referred the papers I propose a new idea i.e. Secure Cross Platform Communication in a cloud. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. Cloud Databases are an emerging type of non relational databases which do not follow relational algebra and are generally key-value oriented systems which are used for storing internet scale data and provide easy programmatic access. The main goal is to securely store and manage data that is not controlled by the owner of the data. The data are stored in cloud environment Cloud security here is solved by providing a Hash Function for data in the cloud.

7. REFERENCES

[1] Shucheng Yu., Cong Wang†, Kui Ren†, Wenjing Lou., "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE

Communications Society for publication in the IEEE INFOCOM 2010.

[2] Loud Security Alliance, “Security guidance for critical areas of focus in cloud computing”, 9, [Online] Available: http:// www.cloudsecurityalliance.org.

[3] Abhishek Parakh, Subhash Kak, "Online data storage using implicit security”, 2009.

[4] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, “Above the clouds: A berkeley view of cloud computing”, University of California, Berkeley, Tech. Rep, 2009.

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services”, IEEE Network, 2010.

[6] Hongwei Li, Yuanshun Dai, Ling Tian, Haomiao Yang, "Identity-Based Authentication for Cloud Computing”, CloudCom 2009, LNCS 5931, pp. 157–166, 2009.

[7] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,“Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[8] H. Shacham, B. Waters, “Compact proofs of retrievability”, in Proc. of ASIACRYPT 2008, vol. 5350, pp. 90–107,

[9] S.Sajithabanu, Dr.E.George Prakash Raj, “Data Storage Security in Cloud”, IJCST Vol. 2, Issue 4, Oct. - Dec. 2011

[10] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing”, 2010.

[11] Tsudik, G. “Message Authentication with One-Way Hash Functions”, Proceedings, INFOCOM’92, May 1992.

[12] Ramgovind, S. Eloff and M.M. Smith, E.,“The management of security in Cloud computing”, in Information Security for South Asia (ISSA), 2010, pp. 1-7.

[13] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta, Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, 2011.