International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

General Article

Data Security in Cloud Computing

K. S. Wagh[A*], Swapnil Chaudhari[A], Anita Deshmukh[B] and Prajakta Khandave[B]

[A]Information Technology, Pune University, Pune-India
[B]Computer Department, Pune University, Pune-India

Accepted 02 May 2014, Available online 01 June2014, **Vol.4, No.3 (June 2014)**

Abstract

Cloud computing is a utilization of computer resources that are available on demand and accessed via a network. A cloud can be a private cloud or a public cloud. A public cloud mainly sells services to anyone on the Internet. A private cloud is actually a proprietary network or a data center that supplies hosted services to a limited number of people. There is a growing trend of using cloud environments for ever growing storage and data processing needs. But still, adopting a cloud computing paradigm may have positive as well as negative effect on data security. Thus we focus on unique feature of the cloud which poses many new security challenges that need to be clearly understood and resolved. So this paper will explore data security of public cloud in cloud computing by implementing digital signature and encryption with public key cryptography.

Keywords: *Cryptography, Encryption, Decryption, Digital Signature, Message Digest.*

1. Introduction

Cloud computing is actually one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services.

What is cloud computing?

Cloud computing is utilization of computer resources that are: Available on demand, Accessed via a network, Charged according to usage, and Provided as a service from a cloud vendor. The various types of deployment model are:
Public cloud - In this the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services. Public cloud services may be free or offered on a pay per usage model. Owned and maintained by the cloud provider.
Private cloud - The cloud infrastructure is operated solely for an organization. The main advantage of using a private cloud is the security, compliance and QoS. Sometime it is risky to put sensitive data outside the organization and premises on a public cloud. Owned and operated by user organization.
Hybrid cloud - The cloud infrastructure is a combination of two or more clouds. It is used when a certain organization is not willing to put its data on public cloud but want to use the financial benefits of cloud data storage private cloud within public cloud. Owned and maintained by a cloud provider.

Contrary to traditional computing practices, in a cloud computing environment, data and the application are controlled by the service provider. This leads to a natural concern about the safety of the data and also its protection from internal as well as external threats. Despite of all these concerns, advantages such as on demand infrastructure, reduced cost of maintenance, pay as you go, elastic scaling etc. are major reasons for enterprises to decide on cloud computing environments. Storing of user data in the cloud despite its advantages has many interesting security concerns which need to be extensively investigated for making it a reliable solution to the problem of avoiding local storage of data.

All these various advantages offered by the cloud can be enjoyed while using services offered by a private cloud by paying some charges but the same thing can be enjoyed by using a public cloud at the least cost or no cost. But using public cloud services also comes with an additional threat regarding the security of data stored at public cloud.

2. Security issues

In a typical scenario where an application is hosted in a cloud, two broad security questions that arises are:
– *How secure is the Data?*
– *How secure is the Code?*
Cloud computing environment is generally assumed as a potential cost saver as well as provider of higher service quality. Security, Availability, Reliability, Data Integrity, Confidentiality, Access control, Authentication are the major quality concerns of cloud service users. In one of

*Corresponding author: **K. S. Wagh**

the prominent challenge among all other quality challenges.

2.1 Security Advantages in Cloud Environments

Current cloud service providers operate very large systems. They have complex processes and expert personnel for maintaining their systems, which small enterprizes may not even have an access to. Due to this, there are many direct and indirect security advantages for the cloud users. Here we present some of the main security advantages of a cloud computing environment:

Data Centralization: In a cloud environment, the cloud service provider takes care of storage issues and small businesses need not spend a lot of money on physical devices for storage. Also, cloud based storage provides a way to centralize the data in a faster and potentially cheaper manner. This is particularly very useful for small businesses, which cannot spend more money on security parameters to secure the data.

*Incident Response***:** IaaS providers can put up a dedicated forensic server that can be used on demand basis. As soon as, a security violation takes place, server can be brought online. In some investigation cases, even a backup of the environment can be easily made and put onto the cloud without affecting the normal course of business.

*Forensic Image Verification Time***:** Some cloud storage implementations expose a cryptographic check sum or hash. For example, Amazon S3 generates MD5 (Message-Digest algorithm 5) hash automatically when you store an object. Thus in theory, the need to generate time consuming MD5 checksums using external tools is eliminated.

*Logging***:** In a traditional computing paradigm by and large, logging is often an after thought. In general, insufficient disk space is allocated that makes logging either non-existent or minimal. However, in a cloud, storage the need for standard logs is automatically solved.

3. Problem Statement

Cloud security is becoming a key differentiator and competitive edge between cloud providers. So by applying the most strongest security techniques and practices, cloud security may soon be more secure than the level that IT departments achieve using their own hardware and software.

A key hurdle to moving IT systems to the cloud is the lack of trust on the cloud provider. The cloud provider, in turn, also needs to enforce strict security policies, which in turn requires additional trust in the clients. To improve the mutual trust between consumer and cloud provider, a good trust foundation needs to be in place. Cloud computing can mean different things to different people. The privacy and security concerns will surely differ between a consumer using a public cloud application, medium-sized enterprise using a customized suite of business applications on a cloud platform, and a government agency with a to cloud systems brings a different package of benefits and risks. What remains constant, though, is the real value that the user seeks to protect. For an individual, the value which is at risk can range from loss of civil liberties to the contents of bank accounts. For a business, the value runs from important trade secrets to continuity of business operations and public reputation. Much of this is quite hard to estimate and translate into standard metrics of value. The task in this transition is to compare the opportunities of cloud adoption with the risks associated with the same.

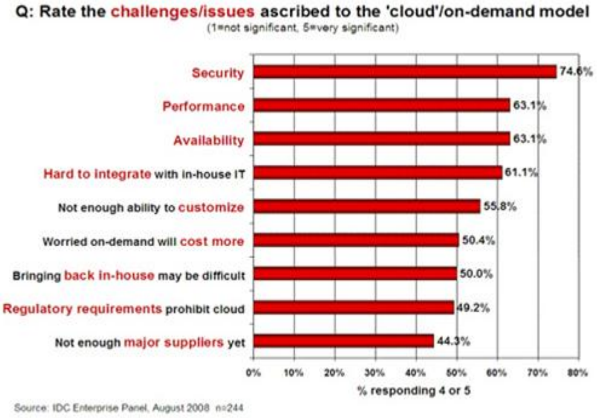
If cloud computing is so great, then why isn't everyone doing it? Because the cloud act as a big black box nothing inside the cloud is visible to client and this leads to two main issues that are :

*Integrity***:** It is degree of confidence that the data in the cloud is protected against accidential or intentional alteration without authorization. Thus it implies that data should be honestly stored on the cloud servers and any violation can be detected.

Privacy: In this concept providers ensured that all critical data example credit card number are masked and only authorized users have access for it. In 2009 a major incident in SAAS cloud happened with Google Docs. Google Docs allows users to edit document online and share these documents with other users. But once these documents shared with any one it was accessible for everyone. Thus in era of personal privacy personal data should really protected.

4. Literature Survey

In 1990 the world was introduced to the internet and we began to see distributed computing power realized on large scale. Today we have the ability to utilize scalable distributed computing environment within the confines of internet, such a practice is known as cloud computing. As we already know there is lots of hype associated with cloud computing.



Source: IDC Enterprise Panel, August 2008 n=244

Figure 2.1: Survey showing issues related to cloud

Cloud computing is a huge topic for that matter please note that we are still discovering many security issues which will challenge to cloud computing because cloud computing is still work in progress and it is rapidly evolving. During a keynote speech to the Brookings Institution policy forum, Cloud Computing for Business and Society,[Microsoft General Counsel Brad] Smith also highlighted data from a survey commissioned by

Microsoft measuring attitudes on cloud computing among business leaders and the general population. The survey found that while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, still more than 90 percent of these same people are concerned about the access, security and privacy of their own data in the cloud.

As we go through the graph of rate of issues and challenges over cloud it shows that security is more demanding as compared to other issues.

The US National Institute of Standards and Technology (NIST), an agency of the Commerce Department Technology Administration, has created a cloud computing security group. This group considers its role as promoting the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards NIST has recently released its draft wide to adopting and using the Security Content Automation Protocol which identifies a quite of specifications for organizing and expressing security-related information in standard ways, as well as related data for reference, such as identifiers for software flaws and security configuration issues. Its application includes maintaining enterprise systems security. In addition to NIST efforts, the industry itself can affect an enterprise approach to security in cloud. But if it applies due diligence and develops a policy of self-regulation to ensure that security is effectively implemented among all clouds, then this policy can also help in facilitating law-making (Lori M. Kaufman *et al*).

Cloud computing is expected to be adopted by the governments, manufacturers and the academicians in the very near future. The author also gives an overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA (Indrajit Rajput *et al*).

There are various unresolved issues threatening cloud computing adoption and affecting the various stake-holders associated with it. The author presents an approach which is aimed at developing an understanding of the security threats that hamper the security and privacy of a user. The various characteristics of a secure cloud infrastructure (public or private) have been discussed and also its challenges and the ways to solve them. The author also highlights various security concerns related to the three basic services provided by a Cloud computing environment and the solutions to prevent them (Amit Sangroya *et al*, 2010).

The author has worked towards facilitating the client in getting a proof of integrity of the data which he wishes to store in the cloud storage servers with bare minimum costs and efforts. The scheme was proposed by the author to reduce the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server (Ashutosh Saxena *et al*, 2011).

Authentication and encryption are suggested for secure data transmission from one cloud to other cloud that requires secure and authenticated data with elliptic curve cryptography. Elliptic curve cryptography has been used to provide confidentiality and authentication of data between clouds (Veerraju Gampala *et al*, 2012).

Cloud environment is considered as a new computing platform to which the classic methodology of security research can be applied. The author determines to employ an attribute-driven methodology to conduct their review (Zhifeng Xiao *et al*).

The author analyses the basic problem of cloud's data security. With the analysis of the architecture of HDFS, they get the data security requirements of cloud computing and set up a mathematical data model for cloud computing (Gu Yaqiang Zhang Quan Tang Chaojing Dai Yuefa *et al*).

5. Proposed Work

5.1 Creating a web application for Campus Management

Initially the Admin of the web portal would verify its users. Student, TPO, HR are the users who access this web application from browser. If the user is verified successfully the admin would approve the particular user by giving him userid and password. After the college TPO or company admin have been approved now the college TPO can in turn approve the college students. All these users access application which is placed over "APPLICATION SERVER". Application server is safe server. All security credentials are stored in application server. It is accessed by trusted person say Third Party Auditor (TPA) after regular intervals of time.

Data of this web application will be stored over "DATABASE" server (public cloud). Data will be transferred from Application server to Database Server. Our motto is to provide security to data transfer from one cloud (i.e application server) to other cloud (i.e database server). We will maintain data integrity and privacy using our strong security mechanism. Data will be encrypted using public Key of database server and sent to database server. Integrity check will be done and safe data will be stored in database server. While retrieving data database server will send data to application server by encrypting data by users public key.

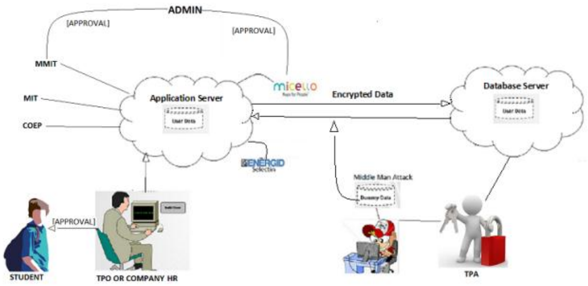


Figure 4.2: Architecture

So if company will have their some selection criteria process that is 60 percent or 50 percent then according to that they will fire the query and will get the list of deserving candidate. Between all these transaction there can be a person or a middle man attacker who can exchange the real data stored on cloud with his dummy data and false information can be provided to the company.

5.2 Online Exam Application

The attacks which can be happen in Online Exam application are

5.1 Attacks on question- Now If candidate is giving an online exam and the questions that the candidate is getting are from public cloud. So there can be a middle man attack where the attacker can access those question and he can change those question. Like if the attacker is in favor of that candidate, then he can change those difficult question into an easier one or vice a versa can also happen.
5.2 Attack on answer- Attacker can also change the answer that the candidate is submitting to the server. Attacker can change the wrong answer into correct answer and correct answer to wrong answer.
5.3 Server Crash- Also it may happen that server may get crash. So we are storing our application in cloud and we are providing security to it by using encryption and decryption algorithm.

So instead of using a traditional way of storing the data, we are creating a replica of our data. So even if server may get crash, then also data is available to us at any time on demand. And we are providing security that is maintaining integrity and privacy of our Online Exam application from all these attack by applying encryption decryption algorithm.

Secure data transfer from Cloud to Cloud

Let us assume that we have two organizations A and B. A and B act as public clouds with data, software and applications. A want to send data to B's cloud securely and data should be authenticated.

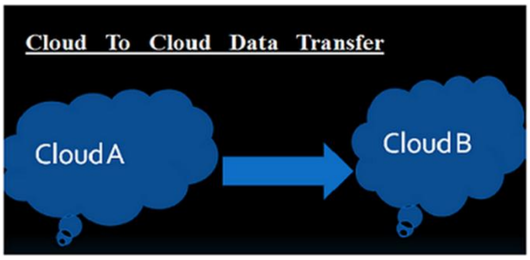


Figure 5.3: Data Transfer

We are here trying to send a secure data from A to B by applying digital signature and data encryption. Suppose B wants an XML document from A's cloud then B's user will place a request to A's user. A's user select corresponding XML document from A's cloud data storage and then apply the hash function, it will give message digest. Sign the message digest with his private key by using A's software. It is called digital signature. Encrypt digitally signed signature with B's public key . Encrypted cipher message will be send to B. B's software decrypt the cipher message to XML document with his private key and verify the signature with A's public key.

Future scope

Our main aim is to provide security. The algorithms we have used will give better privacy. So this can be used in any other applications which are stored on public cloud. Thus we are providing security to public cloud against the various types of possible attacks. This is helpful in Banking applications, Storing criminal data, for Hospital records etc. In the same way even the ERP system for any system could be placed on public cloud.

Conclusions

Thus we have provided security to our application which is stored on public cloud, by using security techniques such as Message Digest, Encryption, Decryption, Hash function. Thus we have successfully maintained the integrity, privacy and confidentiality of our data stored on public cloud.

References

Veerraju Gampala, (2012), Data security in cloud computing with elliptic curve cryptography, *International Journal of Soft Computing and Engineering(IJSCE), 2.*

Zhifeng Xiao and Senior Member Yang Xiao, Security and privacy in cloud computing, *IEEE Communications Surveys and tutorials*, 15.

Lori M. Kaufman John Harauz. Data security in the world of cloud computing. *IEEE Computer and Reliability society.*

Party Auditor Indrajit Rajput. Enhanced data security in cloud computing with third party auditor. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3.

Jens-Matthias Bohli, (July/August 2013), Security and privacy-enhancing multicloud architectures, *IEEE transactions on dependable and secure computing*,10.

Amit Sangroya, (July/August 2010), Towards analyzing data security risks in cloud computing environments.

Ashutosh Saxena Sravan Kumar R, (2011), Data integrity proofs in cloud storage.

Gu Yaqiang Zhang Quan Tang Chaojing Dai Yuefa, (November 21-22, 2009), Data security model for cloud computing

http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.mspx.