RESEARCH ARTICLE OPEN ACCESS

Securing Data Transfer in Cloud Environment

K. S. Wagh*, Rasika Jathar**, Sonal Bangar***, Anu Bhakthadas****
*(Department of Computer Engineering, PUNE University, INDIA)
** (Department of Computer Engineering, PUNE University, INDIA)
*** (Department of Computer Engineering, PUNE University, INDIA)
**** (Department of Computer Engineering, PUNE University, INDIA)

ABSTRACT
Data security and access control is one of the most challenging ongoing research work in cloud computing, due to users outsourcing their sensitive data to cloud providers. The various existing solutions that use pure cryptographic techniques to mitigate these security and access control problems suffer from heavy computational overhead on the data owner as well as the cloud service provider for key distribution and management. Cloud storage moves the user's data to large data centers, that are remotely located, on which user does not have any control. This unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved.

Keywords – Cloud Computing, Decryption, Digital Signature, Encryption, Integrity, Message Digest.

I. Introduction

Cloud computing is a utilization of computer resources that are available on demand and access via a network . These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

Cloud computing is 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. Cloud computing has emerged as the modern technology which developed in last few years, and is considered as the next big thing, in years to come. Since it is new, so it faces new security issues and new challenges as well[1]. In the last few years it is grown up from just being a concept to a major part of the IT industry. Cloud computing is widely accepted as the adoption of SOA, virtualization, and utility computing, it generally works on three type of architecture and these are: SaaS, PaaS, and IaaS. There are different issue and challenges with each cloud computing technology.

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.

II. Security Issues

In a typical scenario where an application is hosted in a cloud, there are two broad security questions that arise :
– How secure is the Data?
– How secure is the Code?

Cloud computing environment is assumed as a potential cost saver as well as provider of higher service quality. Security,

Availability, Reliability, Data Integrity, Confidentiality, Access control, Authentication is the major quality concerns of cloud service users. In one of the prominent challenge among all other quality challenges.

2.1Security 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 access. Thus, 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 storage devices. Cloud based storage provides a way to centralize the data in a faster and potentially cheaper manner. This is 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 in the cloud environment, the 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 considered an afterthought. Allocating insufficient disk space makes logging either non-existent or minimal. However, in a cloud, storage the need for standard logs is automatically solved.

III. Problem Statement

Cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying more stronger 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 and a medium-sized enterprise using a customized suite of business applications on a cloud platform and this 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 protect.

IV. 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.

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[9]. 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, but more than 90 percent of these same people are concerned about the access, security and privacy of their own data in the cloud.

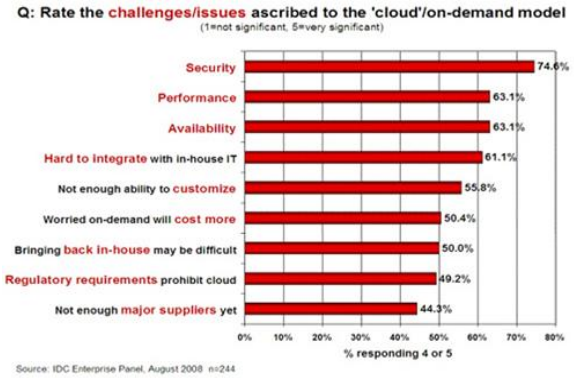

Figure 1: Survey showing issues related to cloud

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.[10]

In [3] the author says that 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, 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 cloud security. If there is application of due diligence and development of 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. By combining industry best practices with the oversight NIST and other entities are still developing, we can effectively address cloud computing future security needs.

In [4] an introduction to cloud computing has been presented that 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.

In [6] the author elaborates the 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.

In [7] 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.

In [1] author suggests authentication and encryption for secure data transmission from one cloud to other cloud that requires secure and authenticated data with elliptic curve cryptography. The author has made use of Elliptic curve cryptography to provide confidentiality and authentication of data between clouds.

In [2] author considers the cloud environment 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.

In [8] 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.

V. Proposed Work

5.1 Creating Web Application For Campus Management

First of all, the Admin of the web portal would verify its users. The users who can access this web application from browser are Student, TPO, and HR. If the user is verified successfully the admin would approve the particular user. 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 secure the 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. While retrieving data database server will send data to application server by encrypting data by respective user's public key.

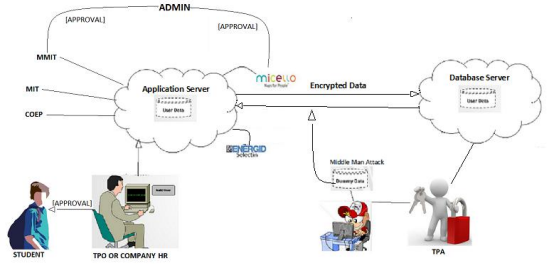

Figure 2: Architecture

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.

5.2Secure 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.

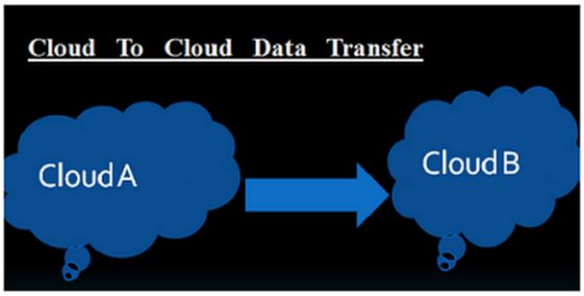

Figure 3: Data Transfer

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.

5.3File Transfer

In File Transfer Module, students can upload their resume, certificates and images while filling students academic information form. Those files will be transmitted in encrypted format and will be stored in cloud in plain text format. Whenever company wants to select the students for recruitment process, they will fire the query based on criteria then they will get the list of deserving students. They can also download the resume of selected student for viewing extra information related to them.

Attacks on File As there is need to provide security to the data, there is also need to provide security to the uploaded file. This is because attacker can attack the file and he will able to do following various types of attacks:-

1. Reading contents of file.
2. Viewing and copying of image present in resume.
3. Attacker can also modify the contents of file.
4. Attacker can misuse the authorized documents like Certificates.

VI. Conclusion

In this paper presented strong security techniques to secure the data files of a data owner in the cloud infrastructure. In our proposed scheme, we have mainly tried to maintain the integrity and privacy of the stored data. The public key, hash, and private key ciphers used between the sender and receiver ensure a secure environment at the cloud. Future extensions include conducting an online aptitude test for the eligible students and providing security to the same.

References

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

[2] Zhifeng Xiao and Senior Member Yang Xiao. Security and privacy in cloud computing. *IEEE COMMUNICATIONS SURVEYS and TUTORIALS*, *15*.

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

[4] 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.

[5] Jens-Matthias Bohli. Security and privacy-enhancing multicloud architectures. *IEEE TRANSACTIONS ON DEPENDABLE AND*

SECURE COMPUTING, 10, JULY/ AUGUST 2013.

[6] Amit Sangroya. Towards analyzing data security risks in cloud computing environments. JULY/AUGUST 2010.

[7] Ashutosh Saxena Sravan Kumar R. Data integrity proofs in cloud storage. 2011..

[8] Gu Yaqiang Zhang Quan Tang Chaojing Dai Yuefa, Wu Bo. Data security model for cloud computing. November 21-22, 2009.

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