GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Analysis of providing security to data on cloud servers

A Project Report of Capstone Project 2

Submitted by

DEEPANSHU MADAN

(1613101245 / 16SCSE101017)

in partial fulfillment for the award of the degree

of

Bachelor of Technology

IN

Computer Science and Engineering

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Under the Supervision of

Dr.P.Muthusamy, M.Tech, Ph.d. (Professor)

MAY 2020

GALGOTIAS
UNIVERSITY

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report **“Analysis of providing security to data on cloud servers”** is the bonafide work of **“DEEPANSHU MADAN (1613101245)”** who carried out the project work under my supervision.

SIGNATURE OF HEAD	**SIGNATURE OF SUPERVISOR**
Dr. MUNISH SHABARWAL,	Dr. P. Muthusamy,
PhD (Management), PhD (CS)	MCA(CS),Ph.D (Cloud Computing)
Professor & Dean,	**Professor**
School of Computing Science & Engineering	**School of Computer Science & Engineering**

Abstract

This project discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The patent will go in to details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications which might already have a security loophole in it. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of guest OS which might have a security loophole in it. This analysis will also provide an insight on data security aspects for Data-in-Transit and Data-at-Rest. The study is based on all the levels of **SaaS (Software as a Service)**, **PaaS (Platform as a Service)** and **IaaS (Infrastructure as a Service).** Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. To guarantee the privacy of information hosted on servers in the cloud, the information could be encrypted which can only be decrypted at the client level with a key.

LIST OF FIGURES

TABLE OF CONTENTS

1. Introduction

i) Overall Description

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment.The cloud is growing continuously because it can provide high performance computational services at cheaper rates. Data security has consistently been a major issue in IT. Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PC's , mobile devices, etc. Data security in cloud computing is more complicated than data security in tradional information systems.To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks.

Cloud computing environment provides two basic types of functions: computing and data storage. In the cloud computing environment, consumers of cloud services do not need anything and they can get access to their data and finish their computing tasks just through the Internet connectivity. During the access to the data and computing, the clients do not even know where the data are stored and which machines execute the computing tasks. Coming to data storage, data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used. A number of data protections and data security techniques have been proposed in the research field of cloud computing. However, data protection related techniques need to be further enhanced.

ii) Purpose

It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. To guarantee the privacy of information hosted on servers in the cloud, the information could be encrypted which can only be decrypted at the client level with a key. Again this is only reliable if the data can be quickly decrypted at the client level as it might need high processing power. The multi-core processors which are evolving will make this possible and provide greater integration of Information. The data is to be encrypted and compressed in multi-server.

iii) Importance of cloud security

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.All cloud models are susceptible to threats. IT departments are naturally cautious about moving mission-critical systems to the cloud and it is essential the right security provisions are in place, whether you are running a native cloud, hybrid or on-premise environment. Cloud security offers all the functionality of traditional IT security, and allows businesses to harness the many advantages of cloud computing while remaining secure and also ensure that data privacy and compliance requirements are met.Now that you understand how cloud computing security operates, explore the ways it benefits your business.

Cloud-based security systems benefit your business through:

- Protecting your business from threats
- Guarding against internal threats
- Preventing data loss

Top threats to systems include malware, ransom ware , and DDos.

Cloud partners offer clear advantages over in-house data storage. Economies of scale allow a cloud service to invest in the latest security solutions, such as machine learning. As cloud solutions are scalable, your business can purchase what you need with the ability to upgrade at any time. Now that you know **what cloud security is**, you have a better understanding of how service providers keep your big data safe. Remember, a strong security policy should outline what strategies the service uses. Security breaches are rarely caused by poor cloud data protection. More than 40% of data security breaches occur due to employee error. Improve user security to make cloud storage more secure. Many factors contribute to user security in the cloud storage system.

2. Existing System (Issues in security of data over Cloud)

Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which need attention and are required to be lined up by making these techniques much better and effective. The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information

The major issues in the cloud computing include **Distributed Denial-of-Service attacks, Insecure API, database privacy and security, system vulnerabilities.** Other issues include **resource security, resource management, and resource monitoring**. Currently, there are no standard rules and regulations to deploy applications in the cloud, and there is a lack of standardization control in the cloud. Numerous novel techniques had been designed and implemented in cloud; however, these techniques fall short of ensuring total security due to the dynamics of the cloud environment. Cloud computing systems can still contain system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms. Once a vulnerability becomes known with a popular third-party system, this vulnerability can be easily used against organizations. Proper patching and upgrade protocols -- in addition to network monitoring solutions -- are critical for fighting this threat. Modern employees may log into cloud solutions from their mobile phones, home tablets, and home desktop PCs, potentially leaving the system vulnerable to many outside threats.

3. Proposed methodology

3.1 Fragmentation Redundancy Scattering Technique

This technique aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system. One way that data manipulation can be reduced is by using strong access controls so that only the authorized users can handle the data. It is also recommended to segregate duties and minimizing access users are given. It is hence crucial for employees to be effectively trained on how to handle the systems. Proper management will also prevent mistakes and ensure that the cloud is secure.

3.2 Digital Signature

The digital signature creation and verification process achieves the subsequent legal requirements:

Signer Authentication

A person’s digital signature cannot be forged except his private key is stolen. This means that if a digital signature can be confirmed by A’s public key, then it must have been created by A’s private key. The digital signature verification process thus validates the identity of the signer.

Message Authentication

A digital signature is constructed upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

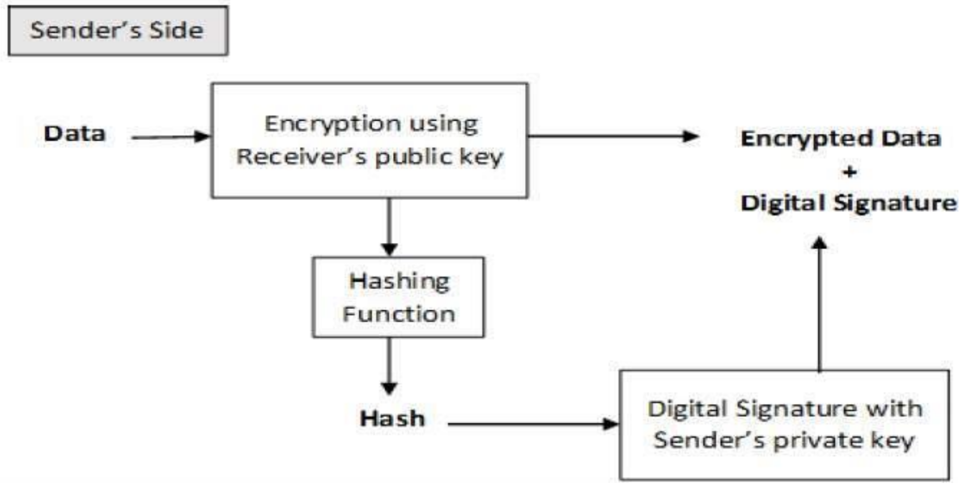
Affirmative Act

The process of digital signature creation involves the signer to use his private key (usually by entering a password). This obvious act alerts the signer that he is initiating a transaction that may have legal consequences

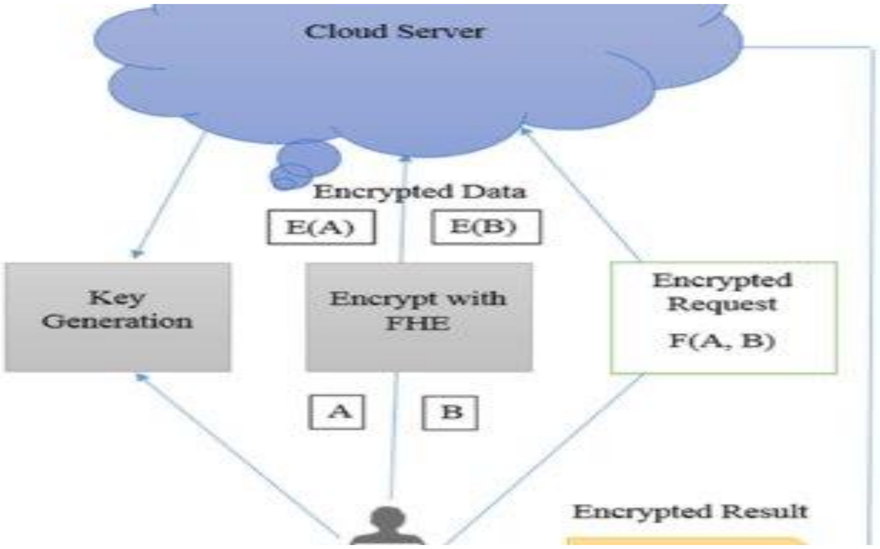
3.3 Homomorphic Encryption

The three basic operations for cloud data are transfer, store, and process. Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider’s premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns. They propose a method based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on cipher texts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication. The authors in provided some real-world cloud applications where some basic homomorphic operations are needed. However, it requires a huge processing power which may impact on user response time and power consumption.

4. Architecture Diagrams


Sender's Side
Data
Encryption using Receiver's public key
Encrypted Data
+
Digital Signature
Hashing Function
Hash
Digital Signature with Sender's private key

Digital Signature Functionality



Encryption model

5. Conclusion

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers.

Cloud computing is a new and promising paradigm to delivering the IT services as computing utilities. Clouds are designed to provide services to external users; providers need to be compensated for sharing their resources and capabilities. In this project, we discussed the problem of security, need of security and what the approaches are needed for application and data security. We have to approach implementing and enforce security issue in SaaS service. The transparency of access data and application use should be authentic with security mechanism. A lot of work already done in the field of security but still, now some security protection already need. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. Cloud computing is recently new technological development that has the potential to have a great impact on the world. It has many benefits that it provides to it users and businesses. For example, some of the benefits that it provides to businesses, is that it reduces operating cost by spending less on maintenance and software upgrades and focus more on the businesses it self. But there are other challenges the cloud computing must overcome People are very skeptical about whether their data is secure and private. There are no standards or regulations worldwide provided data through cloud computing. Europe has data protection laws but the US, being one of the most technological advance nation, does not have any data protection laws. Users also worry about who can disclose their data and have ownership of their data. But once, there are standards and regulation worldwide, cloud computing will revolutionize the future.

6. References

1. Iyer, B. & Henderson, J.C. (2010). Preparing for the future: understanding the seven capabilities of cloud computing. MIS Quarterly Executive, 9, 117-131.

2. Rohan Jathanna Int. Journal of Engineering Research and Application *Vol7, Issue6, (Part5) , June 2017.*

3. Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010

4. Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). December, 2009