Security Issues in Cloud Computing

Saheb K. Gabadia[1], Pritika P. Devadiga[2], Seema Shah[3]

[1,2]Student, Department of Computer Engineering, Mukesh Patel School of Technology Management & Engineering, Mumbai, India

[3]Professor, Department of Computer Engineering, Mukesh Patel School of Technology Management & Engineering, Mumbai, India

***Abstract*: Cloud Computing provides on-demand delivery of services to users. Storage of data is one of the basic services provided by cloud computing. The data is hosted by the cloud service provider on a server and the user can access their data from these servers. The interconnection between different entities such as the data, servers and the data owners need to managed efficiently and faces many security challenges. An entirely different and independent mechanism is required which can ensure that the data is hosted securely and correctly on the cloud server. In this paper, we will discuss the different models in cloud computing and security issues that are faced when the data is hosted on the cloud server and how they can be eliminated.**

***Keywords*: cloud computing**

1. Introduction

Cloud computing provides on-demand services such as data storage to users and organizations and it involves a combination of multiple technologies that have evolved over the years. Many organizations and businesses are moving to cloud technologies because of one main reason: ease of access. The data on the cloud server can be accessed from almost anywhere in the world regardless of the device you use. The devices can range from a basic smartphone to a computer. Cloud computing is being used widely by individuals as well as businesses in day to day life.

Even though most organizations/businesses cloud computing is being used widely, there are some shortcomings due to which individuals or businesses have second thought about using the technology. These issues include security while the data is hosted on the cloud, integrity of data and additional costs in some cases for implementing the cloud. In case of a public cloud, one of the main concerns regarding cloud computing is the that a user may or may not have control over data security. Data security is limited to a certain extent after which data might be leaked or lost.

A very simple solution for preserving data integrity and security is to encrypt the data before uploading it to the cloud and then decrypting it whenever it is to be used. A lot of technologies for data encryption have been developed such as Identity-based encryption (IBE), Attribute-based encryption (ABE), etc. Encryption can be on the client side or server side depending on the type of cloud technology being used. If client-side encryption is used, the data is first encrypted and then sent to the cloud platform. If server-side encryption is used, the data is encrypted and the key is provided by the cloud service provider which can be used to access the data.

The rest of the paper is catalogued as follows: Section 2 Presents an overview of the related work along with the different models in cloud computing [1]. Section 4 encompasses the major security issues in cloud computing. Section 5 contains the conclusion for the paper and Section 6 lists down the references taken.

2. Related Work

Paper 2 discusses the different techniques that are used to secure the data being hosted by the cloud server provider. It highlights the different types of clouds available and the essential characteristics that cloud computing consists of, such as on-demand self-service, broad network access and rapid elasticity. It discusses the use of secure co-processor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. By embedding a secure co-processor (SCP) into the cloud infrastructure, the system can handle encrypted data efficiently [2]. SCP is a tamper-resistant hardware capable of limited general-purpose computations [2]. If tampering is detected, then the secure co-processor clears the internal memory.

Paper 3 talks about considering the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer [3]. It describes, at a high level, the different architectures that combine recent and non-standard cryptographic primitives in order to achieve the goal. It also highlights the benefits that the customers and service providers will get if such an architecture is used. Lastly it gives an overview of the latest advances that have taken place in cryptography, specifically related to cloud computing.

Paper 4 proposes a digital signature method to protect the privacy and integrity of outsourced data in cloud environment [4]. It discusses how a third-party auditor (TPA) can ensure data integrity over out sourced data. In the method proposed above, RSA algorithm for encryption and decryption which follows the process of digital signature for the message authentication [4]. There are three main participants in the method implemented: Third Party Auditor (TPA), User and Cloud Provider. First, the user and TPA generates their own private key and public key with respect to the strong RSA algorithm. The public keys have been shared between them as the part of SLA or in some other ways. Then with respect to the protocol the message is encrypted as well as signed in a unique way [4].

Paper 5 covers various security algorithms related to cloud computing and shows a comparative study on data security algorithms [5]. It covers various encryption techniques such as DSCESEA, SUG-DO (SUGUMARDigits Obfuscation), Advanced Encryption Standard (AES), etc. that have different methods of encrypting data that is uploaded on the cloud and provide data security and integrity in their own way. At the end, all the mechanisms provide some sort of security, although there is still plenty of space to improve results to extract best service from cloud service providers [5].

3. Models in Cloud Computing

There are three cloud computing service models that are used in today's world:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

A. *Infrastructure as a Service*

IaaS, provides business access to various web architecture, e.g. storage space, servers, and connections, without purchasing and managing this internet infrastructure themselves [6]. This benefits both, the user using the service and the service provider providing the Infrastructure to be used. The under lying implementation is managed by the cloud service provider [7]. This service allows the user to install any software or application on the virtual space provided by the cloud. This means that the user can completely manage the storage that is used by them and will be charged for it accordingly.

Some of the key features can be highlighted as follows:

- It saves costs for enterprises of buying and maintaining hardware and equipment as it is completely managed by the IaaS provider.
- There is almost no point of failure as the entire data is on the cloud.
- Monitoring and administrative tasks are virtualized by the cloud which saves up a lot of time for other work.

B. *Platform as a Service*

PaaS is a cloud computing service that delivers application development tools, interfacing tools and other software services that are required for the development of an application software. By providing these tools, PaaS basically delivers an application software over the internet [6]. In PaaS, the infrastructure is provided by the PaaS provider and all the resources needed to use the service efficiently and with ease are also provided by the service provider. The user has to only log in and start using the platform - usually through a web browser interface [6]. The user can easily manage, develop and run an application on the platform with worrying about the equipment's and hardware resources. The platform offers various features such as version management, text editing and testing services that assist the user to make a software efficiently.

Some of the key features can be highlighted as follows:

- Security, server software and backups are managed by the PaaS provider.
- With PaaS, a user can develop, test and host applications in the same environment.
- Organizations can entirely focus on the development part without worrying about the infrastructure, as the PaaS provider manages the infrastructure.

C. *Software as a Service*

SaaS is a cloud computing service where users can access a software based on the cloud which is provided by the SaaS provider itself. The software/application resides on the cloud network which is usually remote, so the users need not install the software/application on the device being used by them. The application can be accessed through the web and it allows users to analyse data in the application and work collaboratively on the project through the application. There are some responsibilities of vendors of SaaS for maintaining software as well as hardware components of applications. They plan and manage redundancy, recovery and data backup and software is updated regularly after some time intervals [6].

Some of the key features can be highlighted as follows:

- Data in the cloud is secured, i.e. hardware failure will not result in loss of data.
- Usability of resources is scalable depending on the requirement of the service.
- Depending on the needs of the services, scalability of resources is available.

4. Security issues in cloud computing

There are various security issues that exist when cloud computing is used. When data is being hosted on the server by the service provider, it has to be made sure that the data is securely uploaded and that data integrity is maintained. Along with this, access to the data on the cloud has to be controlled in such a way that the data is only accessible to the allowed users using mechanisms such as various types of encryptions for the data which can be either provided by the service provided, known as service side encryption or provided by the user itself, known as client side encryption.

Security issues can be broadly categorized as integrity, availability, disaster recovery and confidentiality.

A. *Integrity*

Integrity is a serious problem faced in cloud computing. Integrity of data means to make sure that the data has not been changed by an unauthorized person or in an unauthorized way. It is a method for ensuring that the data is real, accurate and safeguarded from unauthorized users [2].

After storing data to the cloud, user depends on the cloud to provide more reliable services to them and hopes that their data and applications are in secured manner. But that hope may fail sometimes the user's data may be altered or deleted. Sometimes, the cloud service providers may be dishonest and they may discard the data which has not been accessed or rarely accessed to save the storage space or keep fewer replicas than promised [9]. More scenarios for data integrity can include instances where the cloud service provider claims that the data is completely intact and in its original form when actually it is not. Due to these reasons, the users need to be sure about their data being stored correctly in the cloud. There are different methods that have been suggested to preserve data integrity such as Digital Signatures and schemes such as Provable Data Possession (PDP) and Proof of retrievability (PoR) which can be implemented using Message Authentication Code (MAC). MAC is a block of few bytes that is used to authenticate a message. The receiver can check this block and be sure that the message hasn't been modified by the third party [10].

B. *Availability*

Some organizations need their systems to be available all the time because availability is important to them due to the critical services they provide. The cloud services provider offers resources that are shared among many clients. If an attacker uses all available resources, others cannot use those resources, which leads to denial of service and could slow accessing those resources [11]. Another concern that arises is that if there are many people accessing a database at once, some type of denial of service issue for accessing the data may exist which make it unreliable.

C. *Disaster Recovery*

When data is stored on the cloud, it is guaranteed that the data will be available whenever and wherever required by the user. The cloud infrastructure takes care about the data being available even if there are circumstances like power outages but there is a concern here. Even though the concern might be rare, businesses and organizations do consider it before opting for cloud computing. The organization might lose access to all of its IT infrastructure if the cloud service provider is out of business or may be occurring a loss, due to which the entire cloud becomes inaccessible and the organization using it will face significant economic loss as there will be no data available to work on.

D. *Confidentiality*

The major dispute in cloud computing is confidentiality. Data confidentiality means accessing the data only by authorized users and is strongly related to authentication. In another way confidentiality means keeping users data secret in the cloud systems [2]. When a user uploads data on the cloud, controlled access to data is one the most primary needs of the user. The user expects that only the people that have been given access to particular data, access it.

So, for ensuring that the data on the cloud has controlled access, different mechanisms are used. Firstly, the customer should take a stand and ensure application privacy and security. Secondly, trust cannot be outsourced, which is why each organization must own the responsibility to keep its data private [12]. Regardless of the threat, a fundamental building block technology for achieving privacy in a public cloud is data encryption. Cloud encryption allows organizations to build "virtual walls" around their sensitive data, and therefore achieve privacy in a shared environment. But cloud encryption is only one part of the equation. Managing the encryption keys in a shared, public compute environment is the bigger obstacle. Another equally large issue is securing the most sensitive resources, such as the encryption keys themselves, when they are in memory of servers in the cloud [13].

5. Conclusion

Cloud computing allows users to store their data in an isolated location. It has a large number of benefits such as scalability, cost reduction etc. But data security is one of the main concerns in cloud computing due to which cloud computing is not the first option for many individuals or organizations for data storage and other purposes. The paper discusses the various models that cloud computing offers and the major security concerns that are currently present in the technology. The shortcomings can be resolved by various mechanisms, each with different implementations. Data encryption is one the most commonly used data security method, with different levels implemented according to variations of the encryption.

References

[1] Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", EURASIP Journal on Information Security (2016) 2016.
[2] A Venkatesh, Marrynal S Eastaff, "A Study of Data Storage Security Issues in Cloud Computing."
[3] Mahima Joshi, Yudhveer Singh Moudgil, "Secure Cloud Storage."
[4] K. Govinda, V. Gurunathaprasad, H. Sathish Kumar, third party auditing for secure data storage in cloud through digital signature using RSA."
[5] Ramalingam Sugumar, K. Raja, "A Study on Enhancing Data Security in Cloud Computing Environment."
[6] Syed Neha Samreen, Neha Khatri-Valmik, Supriya Madhukar Salve, Pathan Nouman Khan, "Introduction to Cloud Computing."
[7] Vivek Paul, Supriya Pandita, Meera Randiva, "Cloud Computing Review."
[8] Sunita Sharma, "Data integrity challenges in cloud computing."
[9] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, "Cloud Security Issues", in Shacham Proceedings IEEE International Conference on Services Computing, September 2009.
[10] http://www.crypto-it.net/eng/theory/mac.html
[11] Sultan Aldossary and William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions" International Journal of Advanced Computer Science and Applications(IJACSA), 7(4), 2016.
[12] Mayuri R. Gawande, Arvind S. Kapse, "Analysis of Data Confidentiality Techniques in Cloud Computing."
[13] http://www.wallstreetandtech.com/technology-risk-management/the-holy-grail-of-cloud-computing-maint/240006774