International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Data Security in Cloud Computing

Swati Rajaram Karche, Nilima Prakash Jajoo

Student, Department of Computer Science, Sarhad College of Arts, Commerce and Science, Pune, India

Assistant Professor, Department of Computer Science, Sarhad College of Arts, Commerce and Science, Pune, India

ARTICLEINFO

Article History:

Accepted: 25 March 2024
Published: 10 April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
192-198

ABSTRACT

This paper 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 paper 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 security loopholes in them. Similarly, use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might have a security loophole in it. The paper 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)

Keywords : Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

I. INTRODUCTION

The term word Cloud Computing has emerged recently and is not is widespread use. Of the several definitions which are available, one of the simplest is, “a network solution for providing inexpensive, reliable, easy and simple access to IT resources”. Cloud Computing is not considered as application oriented but service oriented. This service oriented nature of Cloud Computing not only reduces the overhead of infrastructure and cost of ownership but also provides flexibility and improved performance to the end user.

A major concern in adaptation of cloud for data is security and privacy. It is very important for the cloud service to ensure the data integrity, privacy and protection. For this purpose, several service providers are using different policies and mechanism that depend upon the nature, type and size of data.

One of the advantages of Cloud Computing is that data can be shared among various organizations. However, this advantage itself poses a risk to data. In order to

avoid potential risk to the data, it is necessary to protect data repositories.

One of the key questions while using cloud for storing data is whether to use a third party cloud service or create an internal organizational cloud. Sometimes, the data is too sensitive to be stored on a public cloud, for example, national security data or highly confidential future product details etc.

This type of data can be extremely sensitive and the consequences of exposing this data on a public cloud can be serious. In such cases, it is highly recommended to store data using internal organizational cloud. This approach can help in securing data by enforcing on-premises data usage policy. However, it still does not ensure full data security and privacy, since many organizations are not qualified enough to add all layers of protection to the sensitive data.

This paper is the study of data security techniques used for protecting and securing data in cloud throughout the world. It discusses the potential threats to data in the cloud and their solutions adopted by various service providers to safeguard data.

The remainder of the paper is organized as follows. Section 2 is the review of literature that provides an insight into the work already done in this area. Section 3 discusses the types of threats to data in cloud. Section 4 examines some efficient data security techniques adopted throughout the world.

The final section is the conclusion which provides summary for this study.

II. LITERATURE REVIEW

In order to understand the basics of cloud computing and storing data securing on the cloud, several resources have been consulted. This section provides a review of literature to set a foundation of discussing various data security aspects.

Srinivas, Venkata and Moiz provide an excellent insight into the basic concepts of cloud computing. Several key concepts are explored in this paper by providing examples of applications that can be developed using cloud computing and how they can help the developing world in getting benefit from this emerging technology.

On other hand, Chen and Zhao have discussed the consumers concern regarding moving the data to the cloud. According to Chen and Zhao, one of the foremost reasons of why large enterprises still would not move their data to cloud is security issues. Authors have provided outstanding analysis on data security and privacy protection issues related to cloud. Furthermore, they have also discussed some of the available solutions to these issues.

However, Hu and A. Klein provided a standard to secure data-in-transit in the cloud. A benchmark for encryption has been discussed for guarding data during migration. Additional encryption is required for robust security but it involves extra computation. The benchmark discussed in their study presents equilibrium for the security and encryption overhead

Tjoa, A.M. and Huemer examine the privacy issue by preserving data control to the end user to surge confidence. Several Cloud computing attacks are reviewed and some solutions are proposed to overcome these attacks.

Therefore, Abdelkader and Etriby propose a data security model for cloud computing based on cloud architecture. They also developed software to enrich the effort in Data Security model for cloud computing further.

III. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

Several risks and security concerns are associated with cloud computing and its data. However, this study will discuss about the virtualization, storage in public cloud and multitenancy which are related to the data security in cloud computing.

A. Virtualization

Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully. A special function called

hypervisor is required to run a guest operating system as a virtual machine in a host operating system.

Virtualization is a foundational element of cloud computing which helps in delivering the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One possible risk is compromising a hypervisor itself. A hypervisor can become a primary target if it is vulnerable. If a hypervisor is compromised, the whole system can be compromised and hence the data.

Another risk with virtualization is associated with allocation and de-allocation of resources. If VM operation data is written to memory and it is not cleared before reallocation of memory to the next VM, then there is a potential for data exposure to the next VM which might be undesirable.

A solution to above mentioned issues is a better planning for the use of virtualization. Resources should be carefully used and data must be properly authenticated before de-allocating the resources.

B. Storage in Public Cloud

Storing data in a public cloud is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud.

In order to avoid such risks, it is always recommended to have a private cloud if possible for extremely sensitive data.

C. Multienancy

Shared access or multitenancy is also considered as one of the major risks to data in cloud computing. Since multiple users are using the same shared computing resources like CPU, Storage and memory etc. it is threat to not only a single user but multiple users. In such scenarios there is always a risk of private data accidentally leaking to other users. Multitenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data.

These types of issues can be taken care of by wisely authenticating the users before they can have access to the data. Several authentication techniques are in use to avoid multitenancy issues in cloud computing.

IV. DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing involves more than data encryption. Requirements for data security depends upon on the three service models SaaS, PaaS, and IaaS. Two states of data normally have threat to its security in clouds; Data at Rest which means the data stored in the cloud and Data in Transit which means data that is moving in and out of the cloud. Confidentiality, and Integrity of data is based upon the nature of data protection mechanisms, procedures, and processes. The most significant matter is the exposure of data in above mentioned two states.

A. Data at Rest

Data at rest refers to data in cloud, or any data that can be accessed using Internet. This includes backup data as well as live data. As mentioned earlier, sometimes it is very difficult for organizations to protect data at rest if they are not maintaining a private cloud since they do not have physical control over the data. However, this issue can be resolved by maintaining a private cloud with carefully controlled access.

B. Data in Transit

Data in transit normally refers to data which is moving in and out of the cloud. This data can be in the form of a file or database stored on the cloud and can be requested for use at some other location. Whenever, data is uploaded to the cloud, the data at time of being uploaded is called data in transit. Data in transit can be very sensitive data like user names and passwords and can be encrypted at times. However, data in unencrypted form is also data in transit.

Data in transit is sometimes more exposed to risks than the data at rest because it has to travel from one location to another. (See Fig 1). There are several ways in which intermediary software can eavesdrop the data and sometimes have the ability to change the data on its way to the destination. In order to protect data in transit, one of the best strategies is encryption.

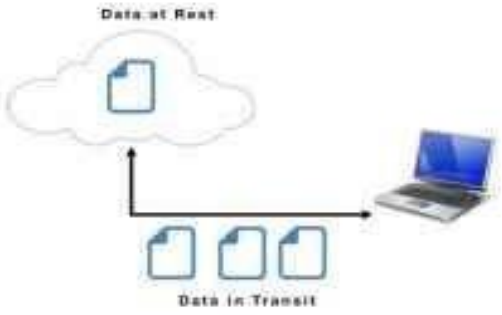

Fig 1: Data at Rest and in Transit.

V. MAJOR SECURITY CHALLENGES

Undoubtedly it is not easy to secure and ensure the safety of linked computers because a series of computers and clients are involved; this is known as multi-tenancy. The cloud service providers and cloud computing have to face many challenges, particularly in the area of security
issues. Thus, it is very important to consider how these challenges are mimicked and how security models are implemented in order to ensure the security of clients and establish a safe cloud computing environment. The major challenges involved are:

• Lack of appropriate governance

During cloud computing the services provider has full control. By passing this control to the provider there is a danger that the loss of control over authority parameters could possibly result in security being compromised, leading to problems in terms of data access and the application of the resources. This compromised security concern comes with another threat of creating a gap in
security cover in cases where Service Level Agreements are not in place with the service provider. Further, the terms of use are also open to the liberty of user meaning that access to data can be exploited quite easily. For instance, the Google search engine states that the user: "agrees that
Google has no responsibility or liability for deletion or failure to store any content and other communication maintained or transmitted through use of the service. Amazon also clearly state that they don't take any responsibility, liability or authority for unauthorized use, corruption, access, loss or deletion of data, or any other sort of access including harm to the application. Hence, customers are faced with security concerns regarding their data and application, as hosted by the third party, service provider or mediator.

• Lock-in

Another hurdle is inadequate standards of data format, a lack of operating methods and shortage of tools which collectively cause compromised portability between the services and applications, even between service providers. Consequently, the customer has to be dependent wholly and solely on
the vendor.

• Isolation failure

The sharing of resources owing to multi-tenancy of cloud computing is itself a questionable characteristic. The shortage of separate storage can be deadly to businesses. Other concerns
involving guest hopping attacks and their problems are considered to be a great hurdle in the use and implementation of cloud computing applications.

• Malicious attacks from management internally

Sometimes the architecture of cloud computing environments poses risks to the privacy and security of the customers.Although it happens rarely, this risk is very difficult to deal with. Examples include the administrators and managers of cloud service providers who can sometimes act as
malicious agents and threaten the security of the clients using cloud computing applications.

• Insecure or incomplete data deletion

In instances where clients request data to be deleted either partially or completely, this raises the question of whether it will be possible to delete the desired part of their data segment with accuracy. This makes it

harder for the clients to subscribe to the services of the cloud-computing.

• Data interception

Unlike with tradition computing, the data in cloud computing is segmented and distributed in transit. This poses more threats due to the vulnerability and fragility of the computing technology and, in particular, sniffing and spoofing, third party attacks and reply attacks.

• Compromise of management interface

Since the services of cloud computing are delivered remotely over the Internet and the
resources are accessible to the service provider, third party access can result in malicious activities. As a result the vulnerabilities, manipulation of services and involvement of the service provider are amplified. For instance, the customer may take over the machines and conversely the provider can take over the control by setting up no-go zones in the applications of cloud computing.

Other challenges related to security include the transfer of information within different applications of cloud computing, leakage of information while uploading data to cloud, attacks on privacy and security of user's data, loss or malicious manipulation of encryption keys and conflicts between service providers and customers on procedure and policies on the operation of cloud computing applications.. There are also challenges that indirectly interact with or influence cloud computing but have no direct impact upon the integrity of cloud computing applications. Such scenarios include: modification of network traffic, network breaks and administrative issues, such as non-optimal use of resources, congestion and miss-connection. There are some other risks
associated to the applications of cloud computing, for instance, the risk of social engineering attacks, natural disasters and theft of equipment.

VI. PROTECTING DATA USING ENCRYPTION

Encryption techniques for data at rest and data in transit can be different. For examples, encryption keys for data in transit can be short-lived, whereas for data at rest, keys can be retained for longer periods of time.

Different cryptographic techniques are used for encrypting the data these days. Cryptography has increased the level of data protection for assuring content integrity, authentication, and availability. In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key as illustrated in Fig 2.

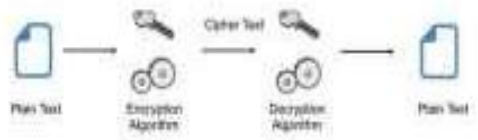

Fig 2: Basic Cryptography Process

Normally there are four basic uses of cryptography:

A. Block Ciphers

A block cipher is an algorithm for encrypting data (to produce cipher text) in which a
cryptographic key and algorithm are applied to a block of data instead of per bit at a time. In this technique, it is made sure that similar blocks of text do not get encrypted the same way in a
message. Normally, the cipher text from the previous encrypted block is applied to the next block in a series. As illustrated in Fig 3, the plain text is divided in to blocks of data, often 64 bits. These blocks of data are then encrypted using an encryption key to produce a cipher text.

B. Stream Ciphers

This technique of encrypting data is also called state cipher since it depends upon the current state of cipher. In this technique, each bit is encrypted instead of blocks of data. An encryption key and an algorithm is applied to each and every bit, one at a time.

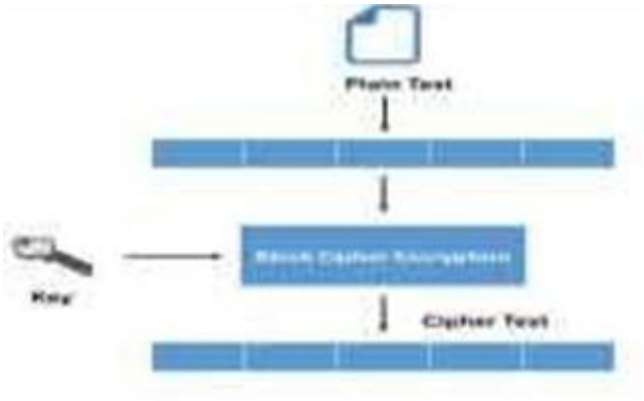

Fig 3: Block Cipher Mechanism

Performance of Stream ciphers is normally faster than block ciphers because of their low hardware complexity. However, this technique can be vulnerable to serious security problems if not used properly.

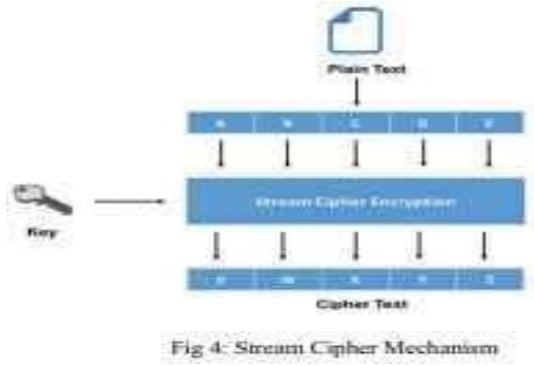

Fig 4: Stream Cipher Mechanism

Fig 4: Stream Cipher Mechanism

As illustrated in Fig 4, stream cipher uses an encryption key to encrypt each bit instead of block of text. The resultant cipher text is a stream of encrypted bits that can be later decrypted using
decryption key to produce to original plain text.

C. Hash Functions

In this technique, a mathematical function called a hash function is used to convert an input text in to an alphanumeric string. Normally the produced alphanumeric string is fixed in size. This technique makes sure that no two strings can have same alphanumeric string as an output. Even if the input strings are slightly different from each other, there is a possibility of great difference
between the output string produced through them.
This hash function can be a very simple mathematical function like the one shown in equation (1) or very complex.

$F(x) = x \bmod 10$ (1)

Fig 5, below shows the mechanism of hash function cryptography.

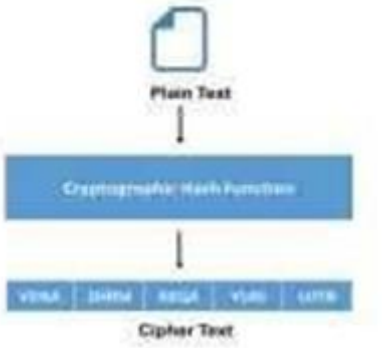

Fig 5: Cryptographic Hash Function Mechanism

All these above mentioned methods and techniques are widely used in encrypting the data in the cloud to ensure data security. Use of these techniques varies from one scenario to another.
Whichever technique is used, it is highly recommended to ensure the security of data in both private and public clouds

VII. CONCLUSION

Increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data in the cloud. Data available in the cloud can be at risk if not protected in a rightful manner. This paper discussed the risks and security threats to data in the cloud and given an overview of three types of security concerns. Virtualization is examined to find out the threats caused by the hypervisor. Similarly, threats caused by Public cloud and multitenancy have been discussed. One of the major concerns of this paper was data security and its threats and solutions in cloud

computing. Data in different states has been discussed along with the techniques which are efficient for encrypting the data in the cloud. The study provided an overview of block cipher, stream cipher and hash function which are used for encrypting the data in the cloud whether it is at rest or in transit.

VIII. REFERENCES

[1]. J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.

[2]. M. A. Vouk, "Cloud computing - Issues, research and implementations," Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.

[3]. P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011.

[4]. A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[5]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[6]. F. Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Netw. Syst. Manag., pp. 562–587, 2012.

[7]. J. Hu and A. Klein, "A benchmark of transparent data encryption for migration of web applications in the cloud," 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[8]. D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[9]. E. Mohamed, "Enhanced data security model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.

[10]. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[11]. V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.

[12]. F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.

[13]. Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[14]. L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012.

[15]. A. U. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, "Security risks and their management in cloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.