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/IJSRSET2411418

Data Security in Cloud Computing

Kumar Kishan Chandra[1], Dr. Manisha Kumari Deep[2]

[1]PhD Scholar, YBN University, Ranchi, Jharkhand, India

[2]Professor, YBN University, Ranchi, Jharkhand, India

ARTICLE INFO

Article History:
Accepted : 02 Sep 2024
Published: 20 Sep 2024

Publication Issue :
Volume 11, Issue 5
Sept-Oct-2024

Page Number :
76-80

ABSTRACT

This article discusses data security issues in cloud computing. It is the study of data in the cloud and its associated security issues. This article will introduce data protection procedures and global practices to insure that data are protected as much as possible by reducing risks and threats. Keeping data in the cloud has been beneficial for many applications, but it creates risks by exposing data to applications that are already weakly secured. Similarly, if the reliability of the guest process (which may have a vulnerability) is unknown when running on a hypervisor, using cloud computing virtualization can lead to the exposure of dangerous information. The white paper will also provide insights into security information in transit and at rest. Learn all levels based on 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 cloud computing has recently emerged but is not widely used. Of the several definitions available, the simplest is "a network solution that provides cost-effective, reliable, simple, and easy access to IT resources." Cloud computing is considered service-oriented rather than application-oriented. The service-oriented nature of cloud computing not only reduces infrastructure overhead and cost of ownership, but also provides convenience to end users and improves performance. The biggest issue with cloud data transfer is security and privacy. Ensuring data integrity, confidentiality and security is critical for cloud services. To achieve this, some service providers use different strategies and methods depending on the nature, type and size of the data. However, this benefit itself also brings risks to the data. To prevent possible threats to the data , it is necessary to protect the data storage. Sometimes important information such as national security information or secret futures is stored in the cloud. . In this case, it is recommended to use the organization in the cloud to store information. This method can help protect data from local data management using policies. However, it is still not possible to ensure data

security and privacy due to the fact that many organizations are not capable of adding all the protection mechanisms for sensitive data in the world. It discusses the threats to data in the cloud and the solutions adopted by various service providers to protect data.

II. LITERATURE REVIEW

We look at several resources to understand the basics of cloud computing and the security of data stored in the cloud. This section provides a data review that forms the basis for discussing various information security issues. This article explores several key issues by providing examples of applications that can be developed using cloud computing and how they can help build a nation that benefits from this new tool. Concerns about moving data to the cloud. Chen and Zhao said that one of the main reasons for the reluctance of large companies to move data to the cloud is security concerns. The authors provide an excellent review of information security and privacy issues related to the cloud. They also discuss some solutions to these problems. The encryption fundamentals for data protection in transit are discussed. To have good security, more encryption is needed, but it requires more computation. The results discussed in their work show the trade-off between security and access overhead. Tjoa, AM Hummer, and Hummer examine privacy issues to provide trust through end-user control over their data. Many air attacks are analyzed , and some solutions are proposed to overcome these attacks. They also developed software to support their further work on cloud computing data security models.

III. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

Many risks and security issues are associated with cloud computing and data. However, in this study, virtualization, cloud storage and multi-location will be discussed in relation to information security in cloud computing.

Virtualization:- Virtualization is a tool that effectively captures the image of work in another work environment to use all real business services. A special feature called hypervisor is required to run the guest operating system as a virtual machine in the host operating system. However, virtualization brings some risks to the data in cloud computing. One risk is that the hypervisor itself could be compromised. If the hypervisor is vulnerable to attack, it could become a prime target. If the hypervisor is compromised, the entire system and data are at risk. If a VM's working data is written to memory and not deleted before the memory is loaded into the next VM, the data will be transferred to the next VM that may not be needed. Ready to use virtualization.

B. Resources should be used with caution and information should be verified before being distributed. Storage in Public Cloud Storing data in public cloud is another security concern in cloud computing. Most clouds use centralized storage, which can be an attractive target for hackers. Storage resources are complex systems that combine hardware and software, if a small breach occurs in the cloud, data can be leaked.

C. Multi-tenancy Multi-tenancy is also considered a major risk for data in cloud computing. Because many users are using the same shared resources such as CPU, storage, and memory. It poses a threat not only to one user but also to many users. In this case, there is always a risk of exposing personal information to other users. Using multiple tenants can be very risky because a problem in the system can allow other users or hackers to access all other files. These problems can be solved by optimizing users before they access data. Use multiple cloud computing technologies to avoid multi-location problems.

IV. DATA SECURITY IN CLOUD COMPUTING

Data security in cloud computing is much more than data encryption. Data security should be based on three service models: SaaS, PaaS and IaaS. There are generally two data security states in the cloud:

1. Data At Rest :-data at rest refers to data stored in the cloud, and data in transit refers to data moving into and out of the cloud. The confidentiality and integrity of information depends on the nature of information protection procedures, methods and procedures. The most important thing is the disclosure of information in the above two states. Static Data Static data refers to data in the cloud or data that is accessible over the Internet. This includes backup files and live files. As mentioned earlier, if an organization does not control the private cloud, it can sometimes be difficult to protect data at rest because they do not have physical control of the equipment. However, this problem can be solved by strictly controlling the access rights of the private cloud.

2. Data in Transit Data in Transit generally refers to data that is being moved in and out of the cloud. This information can be stored in the cloud as files or documents and requested for use elsewhere. When data is uploaded to the cloud, the data at the time of upload is referred to as data in transit. The data in transit may be sensitive data, such as usernames and passwords, that can be encrypted. However, data in unencrypted form is also data in transit . Middleware can eavesdrop on data in many ways, and sometimes modify data as it travels to the destination. One of the best strategies for protecting data in transit is encryption.

V. MAJOR SECURITY CHALLENGES

There is no doubt that it is not easy to protect and secure connected computers because there are computers and clients involved; this is called multi-tenancy. Cloud service providers and cloud computing have to face many challenges, especially security issues. Therefore, it is important to consider how to simulate these challenges and how to use security models to ensure the security of customers' cloud cover. The main problems involved are:

. No good control In cloud computing, the service provider has full control. With this control transferred to the service provider, the lack of permission control poses the risk of compromising security, causing problems in accessing information and using resources. This security protection also brings with it the threat of security inconsistencies if a service level agreement is not made with the service provider. The terms of use are also free for users, which means that access to information can be easily used. For example, the Google search engine, Users: - accept that Google has no responsibility or liability for the removal or failure to store content and other communication communications stored or transmitted through the use of the Services. Amazon also expressly disclaims any liability, responsibility or right for unauthorized use, damage, access, loss or deletion of information or other access (including damage to the Application). Therefore, customers are faced with security issues in data and applications held by third parties, service providers or intermediaries. The portability of applications (and even service providers) is affected. Therefore, customers should trust the suppliers. The lack of independent storage can be fatal for a business. Other problems related to guest attacks and their problems are considered a major problem in the use and usage of cloud applications. Take risks. For example, cloud service providers' administrators and managers can sometimes become criminals and harm the security of cloud users. In the case of partial or complete deletion, this raises whether exactly the necessary part of their data will be deleted. This makes it difficult for users to subscribe to cloud services. This situation increases the threat due to the vulnerability and weakness of technology, especially sniffing and spoofing, third-party attacks and counterattacks. Service providers sent by this method can access the Internet and resources, and third-party access can lead

to malicious activities. As a result, the vulnerability of service providers, service delivery and collaboration are expanding. For example, the customer can host the machine, while the service provider can control the machine by making limited settings in the cloud application. Data leakage when uploading data to the cloud, attacks on users' privacy and security, loss or misuse of encryption keys, and conflicts between service providers and customers go beyond the rules and regulations of operating cloud enterprises. There are some challenges that indirectly affect or affect cloud computing but have no direct impact on the integrity of cloud computing. These factors include: adjustments to network connectivity, network connectivity and resource optimization, management issues such as congestion and network failure. There are other risks associated with air travel, such as social unrest, natural disasters, and the risk of theft.

VI. PROTECTING DATA USING ENCRYPTION

Encryption methods for data at rest and data in transit may differ. For example, for data in transit, the encryption key may be temporary, while for data at rest, the keys will be stored for a long time. Encryption increases the level of data protection to ensure content integrity, authentication, and availability. In its simplest form, cryptography uses an encryption key to encrypt plaintext into cipher text, and then uses a decryption key to decrypt the resulting cipher text, basic encryption:

a. Block cipher :-A block cipher is an algorithm used to encrypt data (to create cipher text); where the encryption key and algorithm are used for the data field, rather than not used. Apply to each child one at a time. This process ensures that similar text in the message is not encrypted in the same way. Usually, the cipher text of the previous encrypted block will be used for the next block in the series. As, the white paper is divided into files, usually consisting of 64 elements. This block of data is then encrypted using encryption keys to create the cipher text.
b. Stream Cipher :-The process of encrypting data is also called state cipher because it depends on the current state of the cipher. In this technology, more than just block data is encrypted. Encryption keys and algorithms are used simultaneously for each bit. However, when used incorrectly, these tools can lead to serious security issues. The resulting cipher text is an encrypted bit stream that can be decrypted using the decryption key to produce the original text.
c. Hash Function :- In this process, the input text is converted into numerical values â□□â□□using a mathematical algorithm known as a hash function. The resulting alphanumeric string is usually fixed in size. This method ensures that no two strings contain the same alphanumeric string as the output. Although the input strings may be slightly different, the output strings they produce will be very different from each other. This hash function can be mathematically very simple, or very complex. All of the above methods and technologies are used to encrypt cloud data to ensure data security. The use of these methods varies from case to case.

VII. CONCLUSION

The increasing use of cloud computing to store information will not necessarily increase the development standards of cloud storage. If you do not properly protect data in the cloud, you may be at risk. This article discusses risks and security threats to data in the cloud and outlines three categories of security issues. Check virtualization for threats from hypervisors. Similarly, threats from public cloud and multi-tenancy are discussed. One of the main topics of this article is information security in cloud computing, its threats, and solutions. Various states of data as well as strategies for encrypting data in the cloud are discussed. This study provides an overview of block

ciphers, stream ciphers, and hash functions used to encrypt objects in the cloud both at rest and 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.

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

[13]. 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.

[14]. 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.