IJMRT: Volume (4), Issue 2, 2022

ISSN (Print):2663-2381
ISSN(Online):2663-4007

International Journal of Multidisciplinary Research Transactions

(A Peer Reviewed Journal)

www.ijmrt.in

Data Security in Cloud Computing

Mr. Kumar Shivam[1*], Mr. Mahesh Nand Kumar Raval[2]

[1,2] Department of MCA, BVUIM, Kolhapur, India.

** Corrosponding Author*

DoI: https://doi.org/10.5281/zenodo.6090321

Abstract

This research basically centers on the data security on Cloud Computing. It could be a consider of information on the cloud and perspectives relating to it for the concern of security. The paper will go in to subtle elements of information assurance strategies and approaches utilized all through the world to guarantee most extreme information security by reducing risks and dangers. Accessibility of information within the cloud is useful for numerous applications but it postures dangers by uncovering information to applications which might as of now have security escape clauses in them. Additionally, utilize of virtualization for cloud computing might hazard information when a visitor OS is run over a hypervisor without knowing the unwavering quality of the visitor OS which might have a security escape clause in it. The paper will to give an understanding on information security perspectives for Data-in-Transit and Data-at-Rest. The ponder is based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

Keywords: Cloud Computing, Data Security, Cloud Computing.

1. Introduction

The term Cloud Computing was developed during the 1960s, Full-time-sharing solutions were available by the early 1970s on various platforms. There is various definition which is available, as one of the best is, "Arrange solution for giving cheap, solid, simple and basic get to to the IT resources" [1]. Cloud Computing isn't considered as application situated but benefit situated. This benefit arranged nature of Cloud Computing not as it were decreasing the overhead of framework and fetched of possession but too gives adaptability and progressed execution to the conclusion client [2],[3]. The major concern is to adoption of cloud for data is security and privacy [4]. It is differentially important for the cloud application service benefit to guarantee the information authenticity, protection and assurance. For this reason, a few benefit suppliers are utilizing diverse approaches and instrument that depend upon the nature, sort and estimate of information. One of the preferences of Cloud Computing is that information can be shared among different organizations. Be that as it may, this advantage itself postures a chance to information. In arrange to maintain a strategic distance from potential chance to the information, it is vital to secure information stores. One of the key questions whereas utilizing cloud for putting away information is whether to utilize a third-party cloud benefit or make an inside organizational cloud. Some of the time, the information is as well touchy to be put away on a open cloud, for illustration, national security information or profoundly secret future item points of interest etc. This sort of information can be amazingly touchy and the results of uncovering this information on an open cloud can be genuine. In such cases, it is exceedingly prescribed to store information utilizing inside organizational cloud. As, this step can help to secure data by implementing on-premises data consumption policy. Although, even now it does not guarantee full data security and privacy, as many organizations are not qualified as much to add all layers of protection to the critical data. This paper is a study of data protection strategies used to protect and secure data from clouds around the world. Discusses potential data threats in the cloud and their solutions adopted by various service providers for data protection. The rest of the paper is arranged as follows. Section 2 is a review of the literature that provides insight into the work that is already being done in this area. Section 3 discusses the types of threats in the data in the cloud.

Section 4 evaluates some of the data security approach that is used across world. The last section concludes this study and it describes the summary.

2. Literature Review

In order to the basics of cloud computing and storing data securing on the cloud, several resources have been Verified. This part describes about the summary of literature to set a structure of emphasizing various points related to data security. Some important concepts are covered in this paper by illustrating though examples of applications that can be developed by using cloud computing and how they can help the developing world to reap the benefits of the developing technology [1]. On the other hand, Chen and Zhao discussed consumer concerns about transferring data to the cloud. According to Chen and Zhao, one of the main reasons why large businesses do not want to transfer their data to the cloud is security issues. The authors provided outstanding analysis of data security and privacy protection issues related to the cloud. In addition, they have discussed some of the solutions to these problems [5,6]. Moreover, Hu and A. Klein provided a set of rules to secure data-in-transit present on the cloud. A benchmark for encryption has been discussed for guarding data during migration. Additional encryption is required for solid security but involves additional computations. The benchmark discussed in their study highlights the equality of security and encryption.

3. Risks and Security Concerns in Cloud Computing

Several risk and security concerns are associated with cloud computing technique. Moreover, this study will emphasize about, Virtualization Storage in public cloud and multitenancy which is related to data security in cloud computing.

3.1. Virtualization

Virtualization is a technique in which a fully functional operating as the system clone is captured in another operating system to utilize the maximum resources of the real operating system. A special function called hypervisor is needed in order to run the guest operating system as a visible device in the host operating system [5,10]. Virtualization is a

basic component of cloud computing that helps bring in the core values of cloud computing. However, virtualization poses some risk to data on a cloud computing. Another potential danger is the hypervisor itself. A hypervisor can be a primary target when it is in danger. If a hypervisor is negotiated, the full system can be negotiated and hence the data [11]. Another risk is with virtualization is concerned with allocation and de-allocation of systems. If VM operation data is burnt into the memory and it is not cleared before reallocation of memory as to the next VM, then there is a strength for data exposure to the next VM which might be unacceptable [12]. The solution to the problems listed above is a better system for using virtualization. Resources must be used carefully and data must be properly verified prior to service withdrawals.

3.2. Storage in Public Cloud

Storing data in a public cloud is another concern for computer security. Clouds often use central storage areas, which can be an attractive target for hackers. Storage systems are complex systems that are a combination of computer and software and can cause data exposure if minor breaches occur in the public cloud[13]. In order to ignore such types of risks, it is always prescribed to have a private cloud if possible for extremely critical data.

3.3. Multitenancy

Shared get to or multitenancy is additionally considered as one of the major dangers to information in cloud computing.[14]. Since different clients are utilizing the same shared computing assets like CPU, Capacity and memory etc. it is risk to not as it were a single client but different clients. In such scenarios there's continuously a hazard of private information inadvertently spilling to other clients. Multitenancy abuses can be outstandingly hazardous because one blame within the framework can permit another client or programmer to get to all other information. [15]. These sorts of issues can be taken care of by admirably confirming the clients some time recently they can have get to to the information. A few verification methods are in utilize to maintain a strategic distance from multitenancy issues in cloud computing.

4. Data Security in Cloud Computing

Data Security in cloud computing involves something more than encryption of data. The need of data security as it totally depends on its three models SaaS, PaaS, IaaS.

Two data regions are often at risk for its security in the cloud; Data on Rest which means data stored in the cloud and Data on Navigation which means moving data in and out of the clouds. Data Privacy, and Data Integrity is based on the nature of data protection methods, processes, and processes. The most significant issue is the broadcast of data in above mentioned two states.

4.1. Data at rest

Rest data points to the data in that is on the cloud, and file related to the data can be accessed directly through Internet. As this includes backup data and live data. As mentioned earlier, it is sometimes very difficult for organizations to protect data when they are at rest if they do not keep the cloud private as they have no real control over the data. However, this problem can be solved by keeping the cloud private with carefully controlled access.

4.2. Data in Transit

Data in transit simply indicates to data which is moving in and out of the cloud. The 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. At any time, data is uploaded to the cloud, the data at the time of upload is called the data along the way. Transportation data can be very sensitive data such as usernames and passwords and can sometimes be encrypted. However, the data is in independent form indicates transport data [17]. Transportation data is sometimes more vulnerable to accidents than data at rest because it has to move from one place to another. There are a number of ways in which link software can listen to data and sometimes have the ability to change data on the way to a destination. To guard transferred data, it is the best encryption method that currently exists.

5. Major Security Challanges

It is some way or another extreme to secure and guarantee the security of connected computers since a arrangement of computers and clients are included; simply known as Multitenancy. The cloud benefit suppliers and cloud computing got to confront numerous challenges, especially within the zone of security issues. Hence, it is exceptionally vital to consider how these challenges are mirrored and how security models are actualized in arrange to guarantee the security of clients and set up a secure cloud computing environment. The major challenges included are: • Lack of suitable administration Amid

cloud computing the administrations supplier has full control. By passing this control to the supplier there's a peril that the misfortune of control over specialist parameters might conceivably result in security being compromised, driving to issues in terms of information get to and the application of the assets. This compromised security concern comes with another danger of making a crevice in security cover in cases were Benefit Level Understandings.

• Lock-in

Another jump is lacking guidelines of information organize, a need of working strategies and deficiency of instruments which collectively cause compromised compactness between the administrations and applications, indeed between fruitful for vendors. Thus, the client has got to be subordinate entirely and exclusively depends on the seller.

• Isolation failure

The sharing of assets owing to multi-tenancy of cloud computing is itself a flawed characteristic. The deficiency of isolated capacity can be dangerous to businesses. Other concerns including visitor bouncing assaults and their issues are considered to be a incredible jump within the utilize and execution of cloud computing applications [20].

• Noxious assaults from administration inside Sometimes the engineering of cloud computing situations postures dangers to the security and security of the clients [21]. In spite of the fact that it happens seldom, this hazard is exceptionally troublesome to bargain with. Cases incorporate the directors and directors of cloud benefit suppliers who can some of the time act as pernicious specialists and undermine the safety for the data through the cloud computing application used by the client.

• Unreliable or partial data deletion

In instances where the client requests the data to be deleted. 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 [22].

• Data interception

Unlike with culture of processing, the data present on cloud computing is segmented and distributed in transit. This ensures more danger because of the vulnerability and fragility of the cloud processing technology and, in particular, sniffing and spoofing, third party application attacks [23].

• Vulnerability of interface

When the benefits of cloud computing are directly delivered through remote manner through the help of Internet and the resources are easily approachable to the service provider, other access can result in vulnerable kind of activities [24]. As a result, involvement of the vendors, vulnerabilities and manipulation of services are amplified. For instance, the customer may take over the machines and conversely the provider can shift the control by setting up barred zones in the applications of cloud computing.

Other hurdles related to security that includes the transfer of resource within different applications or platforms of cloud computing can aims to the 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.[25].

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 conditions includes the changes in network traffic, administrative issues and network loss, such as non-optimal using of resources, congestion and interruption. 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 [26]

6. Protecting Data using Encryption

Encryption strategies for information at rest and information in travel can be diverse. For illustrations, encryption keys for information in travel can be brief lived, while for the information on rest can be held for longer period of time.

Distinctive cryptographic strategies are utilized for scrambling the information these days. Cryptography has expanded the level of information assurance for guaranteeing substance keenness, confirmation, and accessibility. As like in the concept of cryptography, plaintext is scrambled into cipher content by implementing encryption key, and the coming about cipher text is at that point decoded employing a unscrambling key. Normally Cryptography can be divided in three sub types:

A. Secret Key Cryptography.

B. Public Key Cryptography.

C. Hash Functions.

7. Conclusion

Expanded utilize of cloud computing for putting away information is certainly expanding the slant of progressing the ways of putting away information within the cloud. Information accessible within the cloud can be at chance on the off chance that not ensured in a legitimate way. This paper discussed the dangers and security dangers to information within the cloud and given an outline of three sorts of security concerns. Virtualization is inspected to discover out the dangers caused by the hypervisor. So also, the threats occur by Open cloud and multitenancy have been discussed. One of the major concerns of this paper was data security and its dangers and solutions in cloud computing. Information completely different states has been examined in conjunction with the strategies which are efficient for scrambling the information within the cloud. The think about given an outline of square cipher, stream cipher and hash work which are utilized for scrambling the information within the cloud whether it is at rest or in travel.

REFERENCES

[1]. J. Srinivas, K. Reddy, and A, "Cloud Computing Basics," Build. Infrastructure. Cloud Security., vol. 1, no. Sept 2011, pp. 3–22, 2014.
[2]. M. A, "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.
A. Aarthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.
[4]. S. Subhashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Network of Computer. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.
[5]. F. Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Newt. Syst. Manag., pp. 562–587, 2012.
[6]. J. "A Benchmark of Transparent Data Encryption for Migration of Web Applications in the Cloud 8th IEEE Int. Symp. Dependable, Auton. Security. Computer. DASC 2009, pp. 735–740, 2009.
[7]. D. Drescher, 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.
[8]. E. Mohamed, "Enhanced data security model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012. 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.
[9]. V. J. Winkler, "Securing the Cloud," Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.
[10]. F. Sabahi, "Virtualization-level security in cloud computing," 2011 IEEE 3rd Int. Conf. Communication. Softw. Networks, pp. 250–254, 2011.

[11]. Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.
[12]. 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.
[13]. 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.
[14]. T. Mather, S. Kumaraswamy, and S. Latif, "Cloud Security and Privacy," p. 299, 2009.
[15]. F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.
[16]. Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: privacy concerns for consumer cloud storage. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 13). ACM
[17]. Lipinski, T. A. (2013, September). Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements. In International Symposium on Information Management in a Changing World (pp. 92-111). Springer Berlin Heidelberg.
[18]. Ransome, J. F., Rittinghouse, J. W., & Books24x7, I. 2009).
[19]. Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J. (2016). A limited-trust capacity model for mitigating threats of internal malicious services in cloud computing. Cluster Computing,19(2), 647-662. doi:10.1007/s10586-016-0560-2.
[20]. Wang, L., Ranjan, R., Chen, J., & Benatallah, B. 2011).
[21]. Shah, H. and Anandane, S.S., 2013. Security Issues on Cloud Computing. arXiv preprint arXiv:1308.5996.
[22]. Jensen, M., Schwenk, J., Gruschka, N. and Iacono, L.L., 2009, September. On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
[23]. Winkler, V. (. R.)., & Books24x7, I. (2011). Securing the cloud: Cloud computer security techniques and tactics. NL: Syngress Media Incorporated.
[24]. Catteddu, D., & Hogben, G. (2009). Cloud computing risk assessment. European Network and Information Security Agency (ENISA), 583-592.
[25]. H. Qian, J. He, Y. Zhou, and Z. Li, "Cryptanalysis and improvement of a block cipher based on multiple chaotic systems," Math. Probl. Eng., vol. 2010, pp. 7– 9, 2010.
[26]. P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.