DATA` Security in Cloud` Computing

Harshit Parsai
CSE(Hons.)
Sec - RK17TA Rollno. - 09

AIM -> This study describes the security of data in cloud computing. It is about data in the cloud and it's security. The paper details about data protection techniques and approaches used in the world to make sure data is protected by reducing risks. Data present in the cloud is resulting in good for many applications but it may be risky by exposing data to applications which might already have security ambiguity in them.When guest OS is operated on Hypervisor without having knowledge of guest in Virtualisation which may have security risks in it. Term paper also provides an insight on data security aspects for Data-in-Transit and Data-at-Rest. This study is based on Software as a Service and `Platform as a Service and Infrastructure as a Service.

TOPIC COVERED -> Data Security .,Cloud Computing , Data Protection, Privacy, Risks and threats

A. INTRODUCTION -> The Cloud Computing is a network solution for accumulating cheap, able to be trusted, easy and simple access to IT resources Cloud Computing is service aligned.This service aligned nature of Cloud Computing minimizes the expense of infra and cost of right of possessing something also provides flexibility and performance to the end user .Main matter of interest in adaptation of cloud for data is security and privacy . It is important for the cloud service to be sure about the data Integrit , privacy and protection. For this , manyl service providers are using different policies and techniques .One of many advantages of Cloud Computing is that data can be shared among organizations.This advantage itself is a risk to data. In order to avoid risk to the data, it is important to protect data folders and files. One question while using cloud for storing data is if it is worthy to use a third party cloud service or create an inter organizational cloud. occasionally, the data is too private to be on a public cloud, for instance national security data or highly intended to be kept secret for future product details. This data can be sensitive and the result of exposing this data on a public cloud can be harmful . In these cases, it is endorsed to store data in an inter organizational cloud. This approach may help in protecting data by forcing on premises data usage policy However, it does not make sure that data security and privacy, since most organizations are not qualified to add all layers of protection to the sensitive data. This term paper is the study of data security and methods that are used for securing information and data in the cloud from the world. It dictates the threats to data in the cloud and its solutions used by many service providers to safe data. The next parts of the paper are as follows. 2nd Section. is the review of written works that provides an accurate and deep understanding into the work already done in this area, 3rd part discusses the types of damage to data in the cloud. 4th section describes efficient data security methods used by the world. The last part is the conclusion which shows a complete summary for this study.

B. WORK REVIEW -> To understand the basics of cloud computing and storing data securely on the cloud, various resources have been considered. This part is a review of literature to set a foundation of discussion of various data security issues. Srinivas, explained an excellent intuition into the basic concepts of cloud computing. Various key concepts are taken into consideration in this paper by providing some examples of applications that can be built using cloud computing and how they can assist development of the world in getting benefit from this method(technology), Chen and Zhao have given the consumers worry regarding transferring the data in the cloud. Accordingly, one of the reasons why organisations still won't move their data to the cloud is because of security majors. They have discussed data security and privacy protection problems related to the cloud Moreover they have also discussed some of the existing solutions to these issues. Hu and A. Klein overviewed secure data in transit in the cloud A base for en-cryption has been described for saving data during migration. Additional encryption is must for vigorous security but it involves extra computation. The bench provided knowledge in the study for security and encryption . Tjoa, A.M. and Huemer examined privacy issues by saving data control to the end users to sudden confidence Many Cloud computing attacks are reviewed and many solutions are given to overcome attack. As a result Abdelkader and Etriby have given a data security model for cloud computing (cloud architecture) They built software to

enrich the effort in the Data Security model for cloud computing .

C. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING ->

Risks and security worries related with cloud computing and its data. This section will describe virtualization, putting data in public cloud and multi tenancy which are related to the data security in cloud computing.

I. Virtualization Virtualization is a fully functional OS picture captured in other OS to utilize the resources of the real OS. A function called hypervisor is needed to run a guest OS as a VM in a host OS. Virtualization is a part of cloud computing which assists in providing the main values of CloudComputong. Virtualization has some risks to data in cloud computing. One risk is compromising a hypervisor. A hypervisor can become a target if it is at risk. If the hypervisor is compromised, the whole system can be compromised and the data . Another risk with virtualization is with allocating and deallocating resources. If v.m. operation data written. to memory and it is not cleared before re allocation of memory to the next v.m. Then there is a probability for data exposure to the next v.m. which may not be desirable. One solution to this mentioned issue is planning for the virtualization. Resources must be carefully used and data should be properly authenticated. before deallocating resource

II. Storage in Public Cloud Storing -> The Data in a public cloud is security worry in cloud computing Normally cloud implement central storage which can be a target for hacker Storages are complicated system which are consists of h/w and s/w implementation and may cause exposure of data if a slight breach occurs in the public cloud. To avoid such risk, it is recommended to have a private cloud if possible for sensitive data.

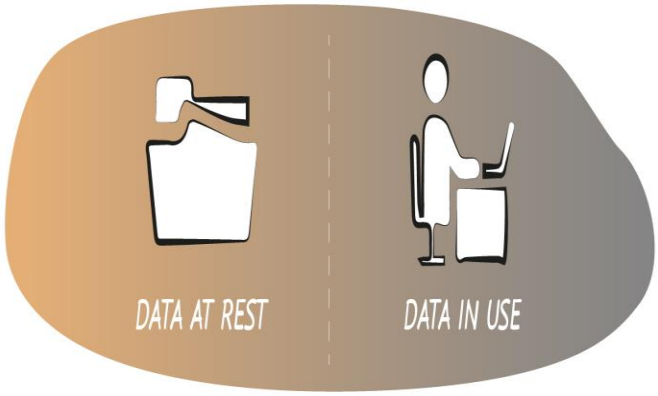
III. Multienancy ->multi tenancy is also considered as one of the major risks to data in cloud computing . Multiple(Many) clients are using the same shared computing resource like CPU, Storages and memory. It is an ultimatum to not only a single user but multiple users. In these scenarios there is always a risk of private data leaking to users. Multitenancy can be risky because one fault in the system may allow other users or hackers to get all data. These types of issues can be taken care of by carefully verifying the users before they can get to the data.Many verification techniques are in use to avoid multi tenancy issues in cloud computing .

D. DATA SECURITY IN CLOUD COMPUTING

-> The Data security in cloud computing is more than data encryptions. Need for data security depends on the three service SaaS PaaS and IaaS. Two states of data normally are in danger to it's security in cloud Data-at-Rest which is the data stored in the cloud and Data-in-Transit which is data that is moved in and out. Confidentiality ,Integrity of data is based on the type of data protection techniques, procedure, and processed. The significant matter is showing data in the above mentioned states.

I. Data at Rest-> Data-at-rest is data in the cloud, any data that can be taken using the internet. This includes backup data and live data. Sometimes it is difficult for enterprises to protect data-at-rest if they are not having a private cloud since they do not have physical control on the data. This problem can be resolved by owning a private cloud with controlled mechanisms and techniques.

II. Data in Transit-> Data in transit is data which is moving in and out. This data can be a file or database stored on the cloud and can be requested for use at some other locations. 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 usernames and passwords and may be encrypted protected at times. There are many ways in which middle software can leak the data and sometimes have the power to change the data in it's way to the destination. so to protect data_in-transit best strategies is encryption



E. MAJOR SECURITY CHALLENGE->

It is not easy to make sure the safety of computers because a series of computers and clients are involved, this is known multi tenancy. The cloud services providers and cloud computing have to face several challenges,In the area of security concern. So it is important to consider how these challenges are considered and how security models are implemented to ensure the security of

clients and make a safe cloud computing environment. The challenges are:

· **Lack of appropriate governance->** In cloud computing the services providers have full control . giving control to the providers there is a possibility that the loss of control over authority parameters could be in security compromisation, leading problems in terms of data access and the application of the resource. These compromised security worries come with another issue of creating a gap in security cover in cases where SLA is not in place with the service providers , the terms of use are also open to the independence of the user means that access to data can be used easily. For example, the Google search engine states that the user accepts that Google is not responsible for deletion or failure to store any content and other communication maintained or transmitted through use of the service . Amazon also clearly stated that they do not take 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 . So, customers are faced with security concerns regarding their data and application, as hosted by the third party service provider.

· **Lock in->** Next problem is insufficient standard of data format, lack of operating method and shortage of tools which together cause compromised portability b/w the service and application, even b/w service providers. the customer has to be dependent on the vendor.

· **Isolation failure->** Sharing resources owing multi-tenancy of cloud computing is questionable. Shortage of separate storage may be deadly to business. Other concern involves guest hopping attack and their problems are considered to be a great obstacle in the use and implementation of cloud computing application

· **Malicious attacks from management internally->** The architecture of cloud computing env. have risk to the privacy and security of the users .it happens rarely, this risk is very difficult to deal Examples include the administrators and managers of cloud service gives access to who can sometime act as bad agents and threaten the security of the client using cloud computing applications.

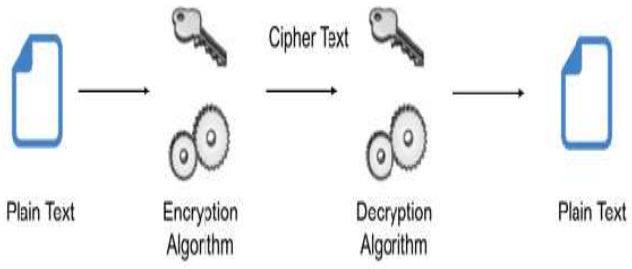
· **Insecure data deletion->** Where users request data to be deleted either partially and completely, raises the question of whether it will be possible to delete the desired part of data collection rightly. This makes it harder for the user to take to the services of the cloud-computing

· **Data Interception->** Unlike with old computing the data in cloud computing is parted and delivered in transport This leads to more threats due to the vulnerability of the computing methods in particular, sniffing and spoofing third party attacks and replay attacks.

· **Compromise of management interface->**Services of cloud computing are distributed distant over Internet , the resources are approachable to the service provider .third party access may result in malicious act As a result vulnerabilities,edit of services and involvement of the service provider are raised. For example the customer may take over the machine and contrarity the provider can take over the controls through setting up no access zones in the applications of cloud computing. Another issue related to security include the movement of information with in different applications of cloud computing leak of information while uploading data to cloud, unauthorised assess on privacy and security of users data loss or malicious edit of encryption key and conflict s between service providers and user on procedures and rules on the operation of cloud computing applications There are also issues that indirectly contact with or influences cloud computing but has no direct effect on the integrity of cloud computing applications These situation include changes of network traffic, network breaks and administrative issues as non optimal use of resources blocking and miss-connection. There are some other issues and warning associated with the applications of cloud computing, the risk of social engineering attacks, natural breakdown.

4. PROTECTING DATA USING ENCRYPTION:->

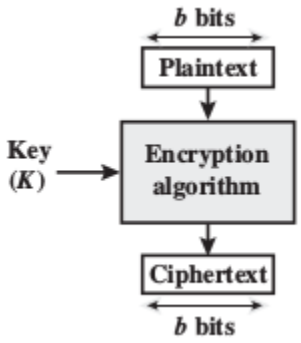
Encryption method for data-at rest and data in-transit are different. For instance, encryption key!s for data-in transit can be temparory may last small, whereas for data- at rest, keys are for long time.



Many cryptography methods used for encrypting data nowadays. Cryptography is an increased level of data protection for making sure content integrity verification and availability.

:Normally there are four basic uses of cryptography:

a. Block Ciphers-> Block cipher is method for making cipher text in which a cryptographic key and algorithm are applied to a blockdata rather than per bit at a time It is made sure that similar blocks of text must not get encrypted in same way in a message.Usually, Cipher text from the last block is applied to the next in a series.



is divided into blocks of data These blocks of data are then encrypted using an encryption _key and produce a cipher .text.

b. Stream Ciphers-> Method of encrypting data is also called state cipher.it depends on the current state of cipher. Each bit is encrypted . An encryption key and an algorithm is applied to every bit. Performance is faster than block ciphers because of less use of hardware complexityThis technique can be vulnerable to serious security problems if not used properly, stream cipher uses an encryption key to encrypt every bit. Produced text is a stream of encrypted bits which can be later decrypted using a decryption key to result the original plaintext.

c. Hash Function->A function called a hash function which is used to convert an input in to alphanumeric string. Resulting alphanumeric strings are fixed in sizes This make sure no two strings can have the same alphanumeric string as a result. Even if the input s are quite different there is a chance of great difference between the output produced through them . This hash function F(z) = z mod 10.

All mentioned methods and algorithms(techniques) are used in encrypting and protecting data in the cloud to ensure data security..Use of the techniques(algorithms) are based on situation . Whichever technique is used recommended to ensure the security of data in private and public clouds.

VII. CONCLUSION-> We have discussed how to store data in the cloud and what the various threads can be there in storing the data in the cloud . We also looked about the various malicious attacks and the security risks that can be there in storing the data in the cloud and how we can make sure the user is free of attacks and the customer data is safe and protected. We have examined the problems related to Data Security in the cloud and how data in the rest and data in transit can be manipulated and how we can protect it using some encryption techniques and hash functions. After this study we are able to understand the protection techniques that are used in the world for instance Block Cipher Stream Cipher and Hash Function are the main techniques used to ensure the data is protected and safe in the cloud.

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. E. Mohamed, “.Enhanced data security model for cloud computing,” Informatics Syst. .(INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.
3. http://www.geeksengine.com/database/design/data-integrity.php.
4. https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp
5. 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.
6. V. J. Winkler, “Securing the Cloud,” Cloud Comput. Secur. Tech. tactics. Elsevier., 2011.
7. Shah, H. and Anandane, S.S., 2013. Security Issues on Cloud Computing. arXiv preprint arXiv:1308.5996
8. M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.
9. F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.
10. 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.

11. 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.
12. Wang, L., Ranjan, R., Chen, J., & Benatallah, B. 2011).
13. F. Yahya, V. Chang, J. Walters, and B. Wills, “Security Challenges in Cloud Storage,” pp. 1–6, 2014.
14. Ransome, J. F., Rittinghouse, J. W., & Books24x7, I. 2009).
15. https://webapps.doe.louisiana.gov/docs/default-source/covid-19-resources/distance-instructional-models.pdf?sfvrsn=9f1f9b1f_2
16. https://link.springer.com/article/10.1186/1869-0238-4-5
17. T. Mather, S. Kumaraswamy, and S. Latif, “Cloud Security and Privacy,” p. 299, 2009.
18. Cloud Security Alliance, “The Notorious Nine. Cloud Computing Top Threats in 2013,” Security, no. February, pp. 1–14, 2013.
19. Catteddu, D., & Hogben, G. (2009). Cloud computing risk assessment. European Network and Information Security Agency (ENISA), 583-592.
20. https://resources.infosecinstitute.com/securely-using-data-in-the-cloud/

THANKYOU :-