Privacy and Security in Cloud Computing: A survey

Saumya Kumar [1], Prof. Harshita Jain[2], Dr.Ritu Shrivastava[3]
[1,2,3]*Department of computer science & Engineering, Sagar Institute of Research & Technology, Bhopal, Madhya Pradesh, India*

***Abstract*— Cloud computing as new technique has developed rapidly in recent time. The problems of security of data over cloud however have caused an enormous impact on the development of cloud and it has also impacted in its popularization, but the importance of cloud and its criticality should not be overlooked. This paper deals with the introduction of cloud computing and different security situation, and it also deal in details about the ways to protect the data and also about the approaches which are being used worldwide to get the maximum protection of data by reducing various risks and threats. Data which are available in the cloud is very much of importance for many applications but it also at the same time poses many risks by the data exposed to applications already having different loophole in its security. Same way, the use of virtualization might add some risk to the data when guest OS is running on top of a hypervisor having no knowledge about the reliability of the running guest OS that might be having security loophole. This paper will too give knowledge on information security perspectives for static data (Data-at-Rest) and Transiting data, and this is based on different level of PaaS, SaaS and IaaS. At last in the paper try to come up with the framework for the cloud computing which can be used effectively for solving the cloud security related problems.**

Index Terms: **Data Security, threats, Data Protection, Privacy, Cloud computing security, Risks, Cloud Computing.**

I.INTRODUCTION

The term cloud computing come in existence very lately. The most simplest definitions from different other are "Cloud Computing is a network solution for providing reliable, inexpensive, simple, and easy provisioning of IT related resources"[1]. The nature of cloud computing is service oriented, The major services provided by cloud is PaaS, SaaS and IaaS.[2] This helps in reducing ownership and infrastructure cost and also helps in providing good performance and flexibility to the user of cloud services[3,4].

The privacy and security of data is of most concern in the use of cloud services. [5]It is most important to ensure privacy, integrity and the protection of the data for cloud. For that very same region many cloud service providers are implementing different mechanism and policies. The mechanism implemented vary with size, type of data and its nature.

Sharing of data among multiple organizations is one of many advantage of using cloud computing. However, at the same time this advantage also poses some risk of data security. To mitigate this risk of data security, protection of repositories where data has been stored is necessary.

The most important question to answer before using cloud storage for the purpose of storing the valuable data is whether we should use private cloud (which is internal to any organisation) or use services of public cloud. When data is very much sensitive such as data related to national security or highly confidential data of industry/company etc. Then storing this type of highly sensitive data on public cloud is very much risky so it is recommended to stored in private cloud in high security.

II.RISK IN CLOUD COMPUTING

A. Virtualization

Virtualization technique allows sharing of the physical instance of single machine/system to utilized by multiple virtual instances. To run guest operating system as VM we require hypervisor. It is one of the fundamental part of cloud computing[6,7]. It also introduces some risk to the cloud computing data. For example one major risk of hypervisor being compromised, and once hypervisor is under control of attacker then whole system and all the data stored in the cloud is exposed to attacker[8].

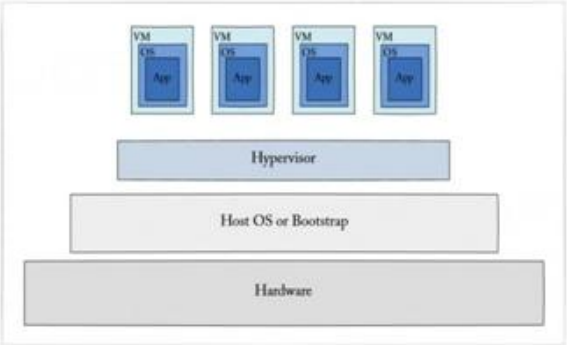

Fig 1: The Cloud's Virtualization [9]

Other risk which is associated with virtualization is allocation and its deallocation of the resources[10]. It occurs when one VM during operation writes some data to the memory and once operation is done same memory space is allocated to other VM without clearing the memory then this leads to the exposer of data to undesirable person which poses a get threat data confidentiality[11]. A solution of this issue is that before de- allocating resource from one VM allocated memory should be cleared.

B. Multitenancy

Term multitenancy refers to the shared access or shared use of same computing resources like Storage, CPU and memory etc[12]. As same resource is being used or shared by different users it poses some short of threat and in this threat all user comes between whom resource is being shared.

In this situation always there is a risk on privacy of data means anyone's data can leak to different user[13]. It can be very much risky because single fault can allow access to all data to another user or attacker. This issues should be handled by using proper authentication of any user who try to access the data. Different techniques can be used for authentication of the user to avoid this issue[14].

C. Public Cloud Storage

Storing your important data on cloud is also a security issue. Generally storage facilities implemented on cloud to store data is centralized system, which is very interesting target for attacker. Resource used for storing data includes both combination of software and hardware, and it is very much complicated. Any instance configuration can cause data exposer and data breach.[15] To avoid this kind of data breach it is advised to use private cloud for very important and sensitive data if possible.

III.SECURING CLOUD

Securing data in clouds involves not only data encryption rather it depends on the cloud service model PaaS, SaaS and IaaS.

Data in cloud remain normally in two state which requires security.

A. Data at Rest

Data at Rest also known as static data which includes data which is stored in cloud or data which is accessed through internet. Some of the data which come under this categories are live data, backup data etc. This kind of data is very difficult to protect. If private cloud is not in use for this kind of data then we do not have any kind of physical control. This kind of issue is mitigated by storing the data in private cloud and applying good access control.

B. Data in Transit

Transiting Data also known as Data in Transit which includes data which is moving either from the cloud or to the cloud, it also includes the data on which computation is going on. The data can be stored in any database or file on cloud and can be fetched from different location. Data in transit poses greater risk then data at rest. It is mainly due to the fact that it has to travel between two location through the unsecured network. There are multiple ways to eavesdrop the packet which is flowing through the network. Also it is possible to make change in the data travelling through the network.[16] This way it poses a great risk of confidentiality and integrity of data. One of the most effective way to protect transiting data is use of encrytpion.

Fig 2: Data at Rest and in Transit [17].

IV. SECURITY PROBLEMS

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content a

A. Failure of Isolation

Multi-tenancy feature or sharing of IT resources of cloud-computing poses some risk to the confidentiality of data. Multi- tenancy helps in minimizing of requirement of separate storage. This feature can also cause different types of attacks such as guest hopping attack etc.

B. Deletion of Incomplete or Insecure Data

In a situation when a client wants to delete any particular data either completely or partially, in such scenario a question arises that is it possible that the desired data or part of it can be deleted accurately. [18].

C. Data Interception

In traditional computing data remain at local system and process of computation is being done locally on that data but in case of cloud computing data remain in transit for quite a long time. This way it makes data vulnerable to different attacks and poses great risk on data. It makes our data available for different attacks particularly sniffing, spoofing and other third party attacks, man in the middle attack and reply attack [19].

V.USING ENCRYPTION FOR PROTECTING DATA

Encryption involves the encoding of the data or message such a way that data or message can only be accessed by authorised parties. The technique used for encrypting static data or data at rest is very much different from the technique used for encrypting transiting data. For examples, encryption keys for the static data is same for longer time period whereas for transiting data encryption key is very short-lived.

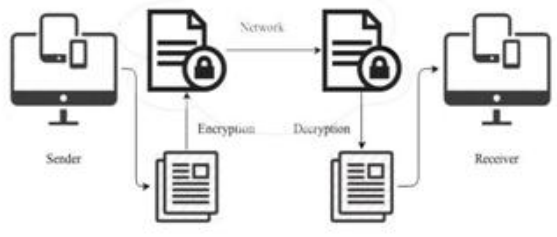

Fig 3: Simple cryptography

Now a days different encryption technique are being used each technique has its own positive points as well as negative points. It is totally dependent upon administrator that which encryption algorithm he/she will use. Cryptography technique has improved the level of protection of data and it has also helped in assuring the authentication, integrity and availability of data. In simple cryptography, plaintext or normal text is encrypted using key known as encryption key and after encryption the encrypted text is known as cipher text and it is then sent over network and then at receiving end cipher text is again converted to plaintext using key known as decryption key[21]. This encryption key and decryption key may or may not be same depending upon the type of encryption algorithm being used.

A. Stream Cipher

As name suggest stream cipher is a technique in plaintext is converted into ciphertext bit by bit means in stream cipher each bit is encrypted one at a time, encryption algorithm is applied on stream of bits.

If we try to differentiate performance wise then stream cipher is faster then block cipher.[20] The region behind the stream cipher being faster then block cipher is because of having low hardware complexity. But if it is not used properly then this can be vulnerable to different security problems.

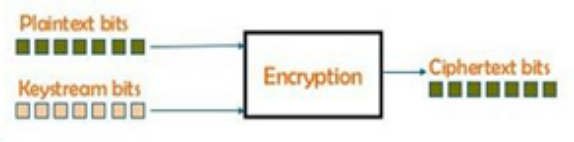

Fig 3:Block Diagram of Stream Cipher[22]

Each bit in stream cipher is encrypted using encryption key. Once encrypted then bit by bit decryption is done on the resultant ciphertext and decryption key is used while decryption process.

B. Block Cipher

Block Cipher is symmetric key encryption technique and it uses deterministic algorithm. Symmetric key encryption means using same key for encrypting plaintext to ciphertext and again for decrypting it. Instead of encrypting single bit at a time like in Stream cipher it encrypts fixed length group of bits at a time. Initially plaintext is segmented into block of

fixed size, generally it is of 64 bits. Then encryption is applied on each block one by one[21].

In Block cipher encryption of similar blocks are not done same way. The cipher text generated from the encryption of previous block is used for next block and it goes on.

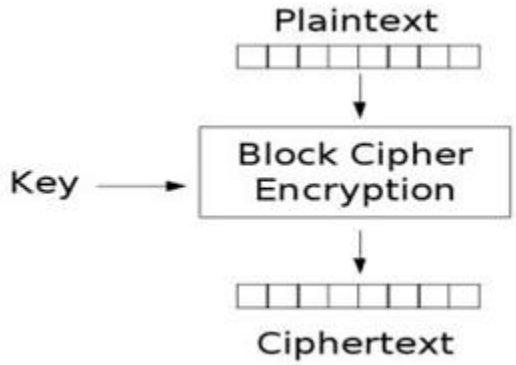

Fig 4: Block Diagram of Block Cipher[23]

C. Hash Function

The Hash Function is pure mathematical function which is used for the conversion of any text into a string containing alphanumeric values. Generally the generated hash value which is in form of alphanumeric character are of fixed length. Also the generated hash value should never be same for any two input text. If there is only minor difference in two input text, then also the hash value of both the input can differ greatly when compared.

The choice hash function depends upon where it is being used. It can be much simplest like shown below in equation

(1) to very much complex like hash function used to store passwords.

$$f(x) = x \bmod 13$$

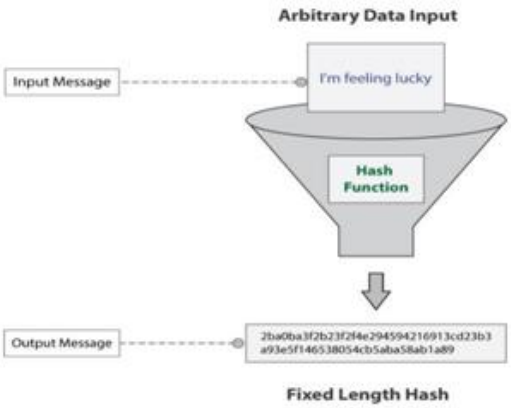

Fig 5: Mechanisim of Hash Function[24]

Hash Function is also known as message digest. It is due to the fact that hash function is non-reversible which means once the hash value is generated from the string then we can not retrieve the string back from hash value. So it is only one way process.

VI. CONCLUSION

Use of cloud-computing is increasing day by day. Now a days almost every person having smart phones uses cloud in one way or another. Major use of cloud services in the field of data storage. Almost everyone store some short of data on cloud to access it from any corner of the world. So that much amount of data is stored on cloud it also attracts the attacker. Which make the data stored in cloud is at risk. My focus in the paper is about the security threats and risk to the data which is stored in cloud and also given some overview about different security concern. Also we try to put forward some of the solution of threat to cloud computing. This paper also give some overview about the stream cipher, block cipher and about hash function. These are some of the technique which is used in cloud for purpose of authentication of user and encryption of data either in transit or at rest.

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] Dikaiakos, M.D., Katsaros, D., Mehra, P., et al.: Cloud Computing: Distributed Internet Computing for IT and Scientific Research 13, 10– 13 (2009)

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

[4] P. S. Wooley, "Identifying Cloud Computing SecurityRisks," Contin. Educ., vol. 1277, no. February, 2011.

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

[6] 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

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

[8] 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.

[9] https://www.w3schools.in/cloud-computing /cloud-virtualization/

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

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

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

[16] F. Yahya, V. Chang, J. Walters, and B. Wills, "Security Challenges in Cloud Storage," pp. 1–6, 2014.

[17] Albugmi, Ahmed & Alassafi, Madini & Walters, Robert & Wills, Gary. Data Security in Cloud Computing. 10.1109/FGCT.7605062, 2016.

[18] 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

[19] 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.

[20] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.

[21] 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.

[22] Tahir, Ruhma & Javed, Muhammad & Cheema, Ahmad.Rabbit-MAC: Lightweight Authenticated Encryption in Wireless Sensor Networks, 2008

[23] https://commons.wikimedia.org/wiki/File:Encryption.png

[24] Tiwari, Harshvardhan. Merkle-Damgård Construction Method and Alternatives: A Review. Journal of Information and Organizational Sciences,2017