International Journal of Engineering Research and Modern Education (IJERME)
ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume I, Issue II, 2016

DATA SECURITY IN CLOUD COMPUTING

Vijayamal S Yakri* & K. Parameshwari**
* Krupanidhi Group of Institutions, Bangalore, Karnataka
** Krupanidhi Degree College, Bangalore, Karnataka

Abstract:

This paper addresses data protection in the cloud. It is a cloud review of data and security-related aspects. The paper will cover the strategies and techniques for data security used worldwide to ensure optimum data safety by reducing danger and hazard. Data available in the cloud is advantageous for certain applications, but it raises challenges as data is exposed to applications that already have safety breakdowns. Similar to that, the use of cloud storage for virtualization could place data at risk as a guest operating system runs over a hypervisor without understanding whether the guest operating system will be protected. It also offers an insight into Data-In-Transit and Data-at-Rest security aspects. The analysis focuses on all levels of SaaS (service software), PaaS (service platform) and IaaS (service infrastructure).

Key Words: Data Security, Cloud Computing, Data Protection, Privacy, Risks and dangers

Introduction:

The word "cloud computing" has recently came into being and is not commonly used. One of the most basic meanings available is a network solution for low-cost, secure, fast and easy access to IT resources [1]. Application-oriented, yet service-focused cloud computing is not yet. This cloud computing services-oriented design not only decreases infrastructure overhead and cost of ownership, but also provides the end user with consistency and increased performance [2, 3]. Security and privacy is a primary issue when applying the cloud to data [4]. For the cloud provider, data integrity, safety and security are essential. To that end, many service providers use various policies and processes based on the nature, type and scale of the information. One of the benefits of cloud storage is that data can be exchanged between different companies. This profit itself however, poses a risk to the data. Data archives must be secured in order to minimize any damage to the data.One of the biggest questions when using cloud to store data is to use a third-party cloud provider or to create an internal cloud. Often data is too important to save in a public cloud, such as national security data or classified product records for the future. These data can be highly vulnerable and can have significant implications for exposure in a public cloud. In such situations, data storage for internal organizational cloud is strongly recommended. This method will help to protect data by applying the data use policies on the premises.However, maximum data protection and privacy are also not ensured, as many organizations are not adequately trained to add all defensive layers of sensitive data.

Literature Review:

Several tools have been consulted to understand the fundamentals of cloud computing and data management in the cloud. This section includes a literature summary that provides a framework for exploring different facets of data protection. Srinivas, Venkata and Moiz give a perfect description of the fundamental principles of cloud computing. In this article, many main topics will be discussed through the provision of examples of apps which can be built using cloud computing and how these new innovations will enable the developing world to benefit from them [1]. The customer issues about transferring data to the cloud have been addressed by Chen and

Zhao on the other side. According to Chen and Zhao, confidentiality problems are one of the key reasons why major corporations don't even transfer their data into the cloud. Authors conducted an exemplary study of cyber storage and cloud-related privacy problems.In addition, some of the solutions available to these problems were also discussed [5, 6]. Hu and A, but. Klein supplied a protocol for ensuring cloud data transit. For data saving during migration, a benchmark for encryption was discussed. For robust authentication, more encryption is needed, but additional computing is required. A balance of security and overhead encryption was addressed in their study [7]. Blues, A. M and Huemer looks at the problem of privacy by maintaining the end user's data access to create trust. Several cloud attacks have been reviewed to address these attacks and several ideas are suggested [8]. Abdelkader and Etriby are also introducing a cloud based data protection model. They have also developed tools to further improve the cloud storage initiative in the data protection model [9].

Risks and Security Concerns in Cloud Computing:

Cloud storage and its data pose many threats and security issues. This analysis would, however, address virtualization, public cloud storage and multitenancy related to cloud data security [3].

- **Virtualization:**

Virtualization is a technique by which an image of a completely operating OS is recorded in another OS to fully exploit the actual OS resources. To run a Guest operating system as a virtual machine on a host function, a special function known as hypervisor is needed [5, 10]. Virtualization is a central concept of cloud computing that helps deliver cloud computing's core principles. Virtualization, however, raises certain risks for cloud-based results. The danger is that the hypervisor itself will be corrupted. If it is vulnerable, a hypervisor can be a primary target. The whole device, and therefore the data [11], can be affected if a hyper vision is corrupted.The allocation and de-allocation of resources is also a risk of virtualization. If VM activity data are written in the memory and not redirected to the next VM until the memory is re-allocated, so there is a possible unintended data exposure to the next VM [12]. A better preparation for virtualization is a solution to the above mentioned problems. Resources can be used carefully and data authenticated accurately before the resources are de-allocated.

- **Storage in Public Cloud:**

Data storage in a distributed cloud is another problem for cloud computing security. Clouds usually run organized servers, and can be an enticing option for hackers. Storage tools are complex structures that incorporate hardware and software that can cause data leakage if the public cloud is partially broken [13]. To eliminate threats, a private cloud with highly sensitive data is often advised.

- **Multitenancy:**

Often called one of the key threats of cloud storage technology is shared access or multi-tenancy [14]. Because many users use the same basic computer resources as CPU, storage and memory, etc, it is not only a concern for a single user, but also for multiple users. There is still the possibility that private data will unintentionally leak to other users in such situations. A device defect will cause a different user or hacker to collect all the other data, which makes multitenance exploits incredibly dangerous [15]. Such problems can be dealt with by the users intelligently authenticated before accessing data is available. Multi-tenancy problems in the cloud machine are avoided by many authentication mechanisms [16].

Data Security in Cloud Computing:

Data protection requires more than data encryption in cloud storage. Data protection specifications depend on the three SaaS, PaaS, and IaaS service models.Data at Rest means data collected in the cloud and transit data that means data going into and out of the cloud; this often means information that usually affects the stability in the cloud. The essence of data privacy mechanisms, protocols and systems are focused on data confidentiality and fairness. The most important thing in these two states is the visibility of the results.

- **Data at Rest:**

The remaining information applies to cloud data or other data available through the Internet. This requires both backup and live details. As previously mentioned, companies often find it very difficult to secure data because they don't keep the private cloud and they don't have physical control of the data. However a private cloud with tightly managed access will address this problem.

- **Transit Details:**

Transit data usually involves data that travels into and out of the cloud. These data may be saved in the cloud and asked to be accessed on another place in the form of a spreadsheet or archive. Once data is transferred to the server, the data is considered data in transit when it is uploaded. The transit data can be very sensitive and can at times be encrypted, such as usernames and passwords. Data are also in transit [17] in non-encrypted form.Data in transit can be more risk-sensitive than data in resting environments because it has to migrate between places. It is possible to retrieve the data in a variety of ways, and to alter it often on the way to the destination. Encryption is one of the best methods for protecting data in transit.

Major Security Challenges:

Certainly, the safe and stable of the attached machines is not easy when there are a range of computers and customers involved. There are several challenges for Cloud services and Cloud Computing firms, particularly in the area of security problems. Therefore the ways these problems are imitated and how security models are applied to ensure customer protection and create a stable cloud storage ecosystem are very important to remember. The biggest obstacles are:

- **Lack of Appropriate Governance:**

The service provider is completely managed during cloud storage. If this control is passed on to the contractor, the concern is that the lack of control of the authority criteria may lead to a breach of protection, resulting in data access issues and the utilization of resources.In the event that service level arrangements with the service provider are not in effect, this breached compliance issue is another possibility of causing a security breach. Furthermore the terms of use are often open to the rights of the user to make it easier to access data. For example, the Google search engine notes that the customer agrees that Google is not liable or responsible for removing or not preserving content and other messages that the use of the site preserves or transmits [18]. Amazon further notes explicitly that they are not accountable, responsible, or responsible for illegal use, corruption, control, failure or elimination of any other kind of data access, like device bias [19]. Therefore users, hosted by a third party, service provider or mediator, face security issues with respect to their data and operation.

- **Lock In:**

Another obstacle is insufficient data format specifications, a lack of operating methods and a lack of instruments which collectively contribute to a compromise of

portability, even between service providers, between services and applications. The buyer must then be entirely and strictly dependent on the seller.

- **Isolation Failure:**

Resource sharing is itself a questionable function due to multitenance cloud computing. The lack of a separate warehouse may be fatal for corporations. Other questions relating to attacks by visitors and their complaints are seen as a big challenge when cloud computing systems are used and introduced [20].

- **Malicious Attack from Management Internally:**

Cloud storage environments often pose a challenge to consumer anonymity and safety [21]. This possibility is very difficult to handle, but seldom exists. Examples include cloud infrastructure controllers and operators, who often behave as malicious agents and who risk consumer protection by cloud storage.

- **Insecure or Incomplete Data Deletion:**

When consumers order data to be partly or entirely deleted, the question arises as to if the appropriate portion of their data section can be correctly deleted. This makes it more difficult for consumers to subscribe to cloud computing services [22].

- **Data Interception:**

Cloud data is not segmented and transmitted in transit, as is conventional computing. The vulnerability and fragility of computation technology particularly sniffing and spoofing, attacks from outside parties and responses, poses more threats [23]. This situation is particularly serious.

- **Compromise of Management Interface:**

As cloud-based services are provided remotely over the internet and the resources of the service provider are available, third-party access may lead to malice [24]. This amplifies bugs, service exploitation and service provider interaction. The user may for example, manage the devices, and the supplier may reverse take control by creating no-go areas in cloud computing applications. Additional security issues include knowledge sharing within different cloud storage applications, data leakage during upload to cloud, privacy and customer data protection threats, failure or malicious misuse of encryption keys and conflicts between service providers or clients on cloud computing operations and policies [25]. There are also threats to the credibility of cloud computing systems that are implicitly interactive with or have some impact on cloud computing. These situations include: network traffic transition, network breakdowns and administrative problems, such as resource loss, encumbrance and mal-connections. Other threats related to cloud computing systems include the possibility of social engineering assaults, natural disasters and equipment theft [26, 29 - 33].

Protecting Data Using Encryption:

Encryption methods could be different for rest data and transit data. For eg, encryption keys may be short for transit data, while keys may be stored for longer periods of time for resting data. Various encryption methods are also in use for data encryption. In order to maintain material confidentiality, security and availabilities, cryptography has improved data protection. Plaintext in the central type of encryption is encrypted into a cypher text with the encryption key and then decrypted with a decryption key. Usual cryptography typically has four basic uses:

- **Ciphers Block:**

A block cipher is an encryption algorithm that uses a cryptographic key and an algorithm for encrypting data (to generate cipher text) rather than per bit at a time [27]. This method means that identical text blocks are not encrypted in a single message in

the same manner. The previous encrypted block's cipher text is usually extended in a sequence to the next block.The simple text is separated into 64 bit data blocks. These data blocks are then scrambled to construct a cipher text using an encryption key.

- **Stream Ciphers:**

This data encryption technique is also known as the state cipher because it relies on the current cipher status. Each bit is encrypted in this technique rather than blocks of info. Each bit is encrypted with a key and an algorithm, one by one [28]. Because of its low hardware complexity, stream ciphers typically work more rapidly than block ciphers. However if not correctly used this technique may be vulnerable to severe security concerns. Stream cipher uses a cryptographic key to encrypt any bit instead of the text block. The resulting text is a stream of encrypted bits, which can later be decrypted to the original plain text using a decryption key [34, 35].

- **Hash Functions:**

In this method, an input text is translated into an alphanumeric string using the mathematical function called a hash function. The alphanumeric string generated is usually fixed in size. It means that no two strings are allowed to have the same alphanumeric string as a production. Even if the input strings vary significantly from each other, the output string generated by them may be very different [36, 37]. Many of these approaches and techniques have been commonly used for cloud data encryption to ensure the confidentiality of data. The use of these methods ranges from scenario to scenario. Regardless of the approach used the protection of data in both public and private clouds is strongly recommended.

Conclusion:

Cloud processing is definitely widely used for data collection, thus strengthening the management mechanisms in the system. If not adequately secured, the data available in the cloud can be dangerous. This paper addressed the dangers and security challenges to cloud data and presented a description of three security issues. In order to define the hypervisor's risks, virtualization is analyzed. Likewise, public-cloud and multimedia-related risks were addressed. The data protection and its threat and solutions in cloud computing are one of the main issues of this article.Data is addressed in numerous states along with strategies for encrypting cloud data efficiently. The analysis presented a description of the block chip, stream chip and hash function used to encrypt the cloud data, whether in rest or transit.

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 andimplementations,” 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 Challengesin Higher Education Institutions,” 2015.
5. S. Subashini and V. Kavitha, “A survey on securityissues 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 LiveMigration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.

7. J. Hu and A. Klein, "A benchmark of transparent dataencryption for migration of web applications in thecloud," 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 ininfrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE, pp. pp. 9–16, 2009.
9. E. Mohamed, "Enhanced data security model forcloud computing," Informatics Syst. (INFOS), 20128th Int. Conf., pp. 12–17, 2012.
10. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutionsat different layers of Cloud computing," J. Super Comput., 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 cloudcomputing," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 250–254, 2011.
13. Cloud Security Alliance, "The Notorious Nine. CloudComputing 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 incloud computing," 4th IEEE Int. Conf. Cloud Comput. Technol. Sci. Proc., pp. 121–128, 2012.
16. T. Mather, S. Kumaraswamy, and S. Latif, "CloudSecurity and Privacy," p. 299, 2009.
17. F. Yahya, V. Chang, J. Walters, and B. Wills,"Security Challenges in Cloud Storage," pp. 1–6,2014.
18. Ion, I., Sachdeva, N., Kumaraguru, P., &Čapkun, S.(2011, July). Home is safer than the cloud!: privacyconcerns for consumer cloud storage. In Proceedingsof the Seventh Symposium on Usable Privacy andSecurity (p. 13). ACM
19. Lipinski, T. A. (2013, September). Click Here toCloud: End User Issues in Cloud Computing Terms ofService Agreements. In International Symposium onInformation Management in a Changing World (pp.92-111). Springer Berlin Heidelberg.
20. Ransome, J. F., Rittinghouse, J. W., & Books24x7, I.2009).
21. Wang, Y., Chandrasekhar, S., Singhal, M., & Ma, J.(2016). A limited-trust capacity model for mitigatingthreats of internal malicious services in cloudcomputing. Cluster Computing,19(2), 647-662.doi:10.1007/s10586-016-0560-2
22. Wang, L., Ranjan, R., Chen, J., & Benatallah, B.2011).
23. Shah, H. and Anandane, S.S., 2013. Security Issues onCloud Computing. arXiv preprint arXiv:1308.5996.
24. Jensen, M., Schwenk, J., Gruschka, N. and Iacono,L.L., 2009, September. On technical security issues incloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
25. Winkler, V. J. R., & Books24x7, I. (2011). Securingthe cloud: Cloud computer security techniques andtactics. NL: Syngress Media Incorporated.
26. Catteddu, D., & Hogben, G. (2009). Cloud computingrisk assessment. European Network and InformationSecurity Agency (ENISA), 583-592.

27. H. Qian, J. He, Y. Zhou, and Z. Li, "Cryptanalysis andimprovement of a block cipher based on multiplechaotic systems," Math. Probl. Eng., vol. 2010, pp. 7–9, 2010.
28. P. Gope and T. Hwang, "Untraceable SensorMovement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.
29. Rajkumar, N & Viji Vinod 2015, 'Integrated Educational Information Systems for Disabled Schools via a Service Bus using SOA', Indian Journal of Science and Technology, vol. 8, no. 13, pp. 1-7.
30. Viji Vinod, Rajkumar, N, Karthikeyan, S & Subramanian, C 2015, 'Expectation of Rising Customer Intelligence System in Road Service Transport using Cloud Services', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 135-142.
31. Subramanian, C, Karthikeyan, S, Rajkumar, N & Sarala Devi, V 2015, 'A Study on Big Data', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 123-134.
32. Subramanian, C, Karthikeyan, S, Rajkumar, N & Sarala Devi, V 2015, 'A Study on Very Large Database', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 114-122.
33. Tamilarasi, R, Rajkumar, N & Karthikeyan, S 2015, 'Evaluating New Server Technology in Midsize Enterprise Markets', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 108-113.
34. Nirmala Sugirtha Rajini, S, Rajkumar, N & Mercy Beulah, E 2015, 'An Innovative Cloud Computing Infrastructure for e-Tourism', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 19-22.
35. Subramanian, C, Rajkumar, N, Karthikeyan, S & Vinothkumar 2015, 'List Based Scheduling Algorithm for Heterogeneous System', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 1-6.
36. Gohin, B, Viji Vinod & Rajkumar, N 2012, 'Cloud Computing Architecture for Visual Disabilities on E-Governance', International Journal of Computer Applications, vol. 52, no. 1, pp. 44.48.
37. Gohin, B, Viji Vinod & Rajkumar, N 2012, 'Usability of Cloud SaaS based E-Governance for people with Disabilities', International Journal of Computer Applications Proceedings on E-Governance and Cloud Computing Services – 2012, vol. 2, no. 2, pp. 23-28.