DOI: http://dx.doi.org/10.26483/ijarcs.v15i6.7162

Volume 15, No. 6, November-December 2024

ISSN No. 0976-5697

nternational Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A STUDY OF SECURITY AND STORAGE OF DATA IN CLOUD COMPUTING ENVIRONMENT

Priyanka Verma
Research Scholar, NIILM University,
Kaithal,India

Pawan Kumar
Assoc. Professor, NIILM University,
,India Kaithal

Abstract: In cloud environment, the cloud data security plays an essential role in order to properly handle and access the data on cloud storage server. The protection of cloud data from the unauthorized user is a challenging task due to the lack of user authentication and authorization in cloud. The keyword extraction is the easiest way to extract the required documents/files relevant to the searched keywords. Many researchers have been focused on the providing secured keyword search to access data stored on cloud storage by introducing security protocol, cryptography techniques include encryption and decryptionalgorithms.

Keywords: Cloud, Cryptography.

1.INTRODUCTION
SECURITY AND STORAGE OF DATA

In today's world of infrastructure protection (network, server, and application level), data security is becoming more critical as cloud computing is used at all levels: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). There are several security aspects of the data, including:

- In-transit details
- On-rest data
- Data collection, including the multi-tenancy
- Lineage Details
- Provenance of Data
- The remanence of data

This is designed to aid consumers in assessing their data security situations and to measure the vulnerability of their organizations. Not all in these topologies has the same value as in other fields of cloud storage and security (for example, the usage of a public cloud versus a private cloud or the use of insensitive data versus sensitive data).

2.ASPECTS REGARDING DATA SECURITY

There is no accepted encryption method as to the primary danger of data in transit. Though this is apparent to ISPs, it is not normal for anyone to be conscious of this situation while utilizing a public cloud irrespective of whether it's IaaS, PaaS or SaaS. It is also important to ensure the protection of secrecy and dignity of a protocol especially when the protocol is used to send data over the Internet (for example, the FTP over SSL, the Hypertext Transmission Protocol Safer HTTPS and the Protected Copy System SCP). Data protection alone can offer security and does not protect data privacy with the usage of an unsecured protocol (e.g. normal FTP or HTTP).
While encryption may appear simple to use to protect the data on residue, the truth is not that straightforward. If you are utilizing an IaaS cloud provider (public or private) for convenient storage (e.g. Amazon Basic Storage or S3), it is necessary to use dataat rest encryptions which is strongly recommended. The dataatrest used by a PaaS or SaaS cloud system (e.g. Google Apps or Salesforce.com) cannot often be encrypted as a reimbursement tool, though generally, the cloud-based program does not encrypt dataatrest, which avoids indexing or scanning of such details.
Generally speaking, cloud computation of data at rest has the benefit of utilizing a multi-variety Model for PaaS-based software and SaaS. In other terms, whether data is being analyzed or collected for usage in a cloud-based program with data from other users (that is, normally held in a massive data store such as Google BigTable). The data should be mixed with data from other users. While apps are sometimes configured to avoid unauthorized access to mixed information, such as data tagging (for additional specifics, SaaS application security), unauthorized access is always possible by any manipulation of an application weakness. Data is not of a single organization on one network whereas other cloud services monitor third-party apps or verify the protection capabilities of third-party applications.
While a company's data transfer is compressed and authenticated via basic storage (i.e. while not attached to a single application) throughout the move from and to a cloud service, the data residue cannot be encoded, business knowledge will definitely not be encrypted because it is retained in the cloud (public or private). For some device manipulation of the data, the data must be unencrypted. Until June 2009, the complete transmission of cryptographic data was not documented. If the information is actually processed in the cloud, the data must then be encrypted for at least half of its life span in the cloud and at least for encryption purposes.
IBM announced in June 2009 that one of its researchers has established a fully homomorphic encryption system that allows data to be stored without decryption, collaborating with a post-graduate student of Stanford University.This was a major advancement in the field of cryptography and would have an enormously beneficial impact on cloud storage as long as it is applied. In previous work on purely homomorphic encryption,

Stanford University has made an announcement from IBM that fruitful studies had been improved. Although the theoretical barrier to totally homomorphic encryption was overcome by a homomorphic device, considerable computational work was needed. Ronald Rivest (MIT professor and coinventor of the famous RSA encryption scheme) notes that the steps to render it operable would not be far behind. Another cryptographic activity is underway to minimize details, such as predicate encryption, that will need to be decrypted for cloud computing.

It is convenient and important to know exactly when and where the data has been processed specifically inside the server, whether the data contained in the server are authenticated or not, (for verification or regulatory purposes). For example, the data may have been moved to a cloud provider, such as Amazon Web Services (AWS), on date x1 at time y1 and stored in a bucket on Amazon's S3 in example 1.s3.amazonaws.com, then processed on date x2 at time y2 on an instance used by an enterprise on Amazon's Elastic Computing Cloud (EC2) in ec2-67-202-51-223.compute-1.amazonaws.com, then restored to another bucket, exazonaws.com. The data trace (mapping of application data flows or simulation of data paths), which is known as the data trail, is essential for auditor verification (internal, external and regulatory). However, it takes time to provide auditors or administrators with data background, particularly if the system is primarily managed by an individual. It is just not feasible to seek to provide a public cloud provider with accurate data lineage documentation. What physical layout does the bucket supply in example1.s3.amazonaws.com, and where exactly is the container (or was it) in the previous example? What was the condition of the body then and how could a client or an inspector regulate the knowledge?And though it is feasible to set up a data route on a public cloud, certain clients also have a far more overwhelming need to prove data source not only proving the authenticity of the results, but also proving the quality of their sources. Both definitions vary considerably. For data not illegal or harmful, data honesty exists.Provenance not only denotes authenticity of the results, it also indicates consistency of calculation, in other words precise analysis of the data. Consider, for starters, the following financial equation:

$$((2 * 3)*4)/6)-2) = \$2.00$$

The solution to this question is valued at $2.00. There would be a question of fairness if the result were specific. For example, it is assumed that $2.00 is in US dollars, but the inference may be inaccurate if a certain currency is used with the accompanying assumptions:

- Australian dollars, Bahamian dollaries, Barbados dollars, Belizean dollars, Cayman Islands, Cayman Islands, Canadians, Cook Islands, East Caribbean dollar, Fijian dollars, Kyribati, Jamaican dollars, Liberian Dollars, Namibian dollars, New Zealand dollars, Samoy, Tuvak dollars or Zimbabwe.
- The currency will be converted from another country's dollars into US dollars.
- A valid exchange rate is used and accurate calculation and clarification of translation is necessary.

In this case, the equation has a meaning which has no basis because it satisfies those requirements. In certain real-life scenarios there is insufficient data transparency, and data source is critical as well. Two simple sources are financial and science estimates. When utilizing common resources in a cloud setting, how can you show data provenance. You will not be able to track the networks or environment they use at the moment, but you know some computer identity information (eg IP addresses of devices) and their general status (e.g., a country, even a data center). Such facilities are not under your physical or even conceptual influence.

The remanence of data is a final component of data security. The data residue is the residual picture of data that was nominally removed or deactivated in any manner. It is possible to disclose confidential details inadvertently by exposing the data in an uncontrolled environment, either through an intact removal procedure or the physical properties of the storage medium.

There is an unintentionally unwanted group to threaten the data remanence on cloud services whatever cloud software you use (SaaS, PaaS or IaaS). In certain situations, the data may be leaked in the web. The risk of SaaS or PaaS is almost probably unintentional or unintended contact. However, this does not guarantee potential consumers after unauthorized release and may question the resources or reviews used by third parties for checking the security of the apps or network of the provider.

Despite the increasing value of data security, cloud service providers (CSPs) are paying very little attention to data remanence. Many may not even think that their systems are remanent with results. And several CSPs are having a really positive commitment to US enforcement when it comes to data security. Defense Department (DoD) 5220.22-M (National Workplace Security System Operating Manual). DoD 5220.22-M sets out the two agreed data (destruction) methods, but does not define any specific conditions for the operation of these two methods or any guidance on how they should be carried out. This 141-page DoD 5220.22-M handbook has only three sub-sections for important details concerning remanence. Accrediting Cognizant Security Agency (CSA) shall issue guidelines on the processing, sanitization, and release of information systems (IS) media.Clearing is the way medium-data is eradicated before media are reused in an environment where computer protection before clearing is sufficient. In order to avoid successful exposure to previously recorded material, the internal memory or buffer must be transparent.Sanitization is the way to remove data from media before re-using media in a setting where data protection is not sufficient until sanitization. Until the classified restrictions on knowledge are withdrawn or open for usage in a lower level, IS tools have to be sanitized.

Providers will see a specific Publication of NIST, 800-88 "Online Sanitation Guidelines. " While this NIST publishing gives advice only, which is officially only reserved for federal civil departments which departments, many organizations, particularly those in enforcement, can have comprehensive details about the way data security is to be accomplished. In the absence of any other industry standard for data remanence, it is important to follow these NIST guidelines

3.CONCLUSION

The cloud storage service is established over an internet, depending on the virtualized infrastructure with accessible interfaces, near-instant elasticity, multi-tenancy, scalability and metered resources. Within logical pools, the data is stored on the cloud in diverse and disparate, commodity servers placed in premises or at a data center maintained by a third-party cloud service provider. The main purpose of cloud storage is to ensure that the user can access data from anywhere on the cloud. The major advantage of cloud storage is the universal access to documents, improved data reliability and easier collaboration between groups. The cloud storage is used to store personal data, share data between two entities, and distribute specific information within manufacturing companies.Ventures are progressively embracing cloud storage alternatives since they need greater limit, versatile limit and a superior method to oversee storage costs after some time. The growth of big business data and cloud data are making hard for IT offices to store data at their place alone.

REFERENCES

1. S. Kamara, C. Papamanthou, and T. Roeder, 'Dynamic searchable symmetric encryption',in Proceedings of the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 2012, pp. 965–976
2. X. Ge, J. Yu, H. Zhang et al., 'Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification', IEEE Transactions on Dependable and Secure Computing, 2019, pp. 1–16.
3. Cheng-Kang Chu., Sherman S. M. Chow., Wen-Guey Tzeng, Jianying Zhou., and Robert H. Deng., „Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage,‟ IEEE Transactions on Parallel and Distributed Systems, vol. 25, No. 2, February 2014, pp. 468 – 477.
4. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, „Privacy-Preserving Public Auditing for Secure Cloud Storage‟, IEEE Transactions on Computers, vol. 62, No. 2, February 2013, pp. 362 – 375.
5. D. Chandramohan , T. Vengattaraman, D. Rajaguru and P. Dhavachelvan, „A new privacy preserving technique for cloud service user endorsement using multi-agents‟, Journal of King Saud University - Computer and Information Sciences, Elsevier, vol. 28, No. 1, January 2016, pp. 37-54.
6. Daniel Díaz-Sánchez, Florina Almenarez, Andrés Marín, Davide Proserpio, and Patricia Arias Cabarcos, „Media Cloud: An Open Cloud Computing Middleware for Content Management‟, IEEE Transactions on Consumer Electronics, vol. 57, No. 2, May 2011, pp. 970-978.
7. Deepa P L, S Vinoth Kumar and Dr S Karthik, „ Searching Techniques In Encrypted Cloud Data‟, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) vol. 1, No. 8, October 2012, pp. 1-5.
8. Guojun Wanga., Qin Liu., Jie Wub., Minyi Guo., Science Direct., Elsevier Journal., „Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,‟ Computers & Security, Elsevier, vol. 30, No. 5, July 2011, pp. 320-331.
9. Gurpreet Singh and Supriya Kinger, „Integrating AES, DES, and 3- DES Encryption Algorithms for Enhanced Data Security‟, International Journal of Scientific & Engineering Research, vol. 4, No. 7, July 2013, pp. 2058- 2062.
10. Hongwei Li,Dongxiaoliu,Yuanshun Dai, Tom H. Luan and Xuemin(Sherman) Shen, „Enabling Efficient Multi-Keyword Ranked Search over Encrypted Mobile Cloud Data through Blind Storage‟,IEEE Transactions on Emerging Topics in Computing, vol. 3, No. 1, March 2015, pp. 127-138.
11. Z. Fu, X. Sun, S. Ji, and G. Xie, 'Towards efficient content-aware search over encrypted outsourced data in cloud', in Proceedings of the 35th Annual IEEE International Conference on Computer Communications, INFOCOM 2016, vol. 1–9, San Francisco, CA, USA, April 2016.
12. X. Ge, J. Yu, C. Hu, H. Zhang, and R. Hao, 'Enabling efficient verifiable fuzzy keyword search over encrypted data in cloud computing', IEEE Access, vol. 6, 2018, pp. 45725–45739.