ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Data Security in Cloud Computing: A Survey

Tarasvi Lakum, B.Thirumala Rao*

Research Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India,
* Professor, Department of CSE, Lakireddy Bali Reddy College of Engineering, Mylavaram, India

ABSTRACT: Cloud computing is one of the fastest emerging technologies in computing. Cloud Computing applies as a software on-demand remotely to the usage of machine services. This is primarily focused on data and software outsourced to remote repositories (datacenters), which are typically housed on consumer machines and are operated by third parties. This paper provides an analysis of cloud storage, security problems. This seeks to address the key data security concerns posed by the cloud world. These questions were then classified into three categories: 1-data security concerns occurring in relation to conventional infrastructures with the single cloud containing features, 2-data security issues posed in cloud storage across the application life cycle (data processed, utilized and transferred), 3-data security issues correlated with data security qualities, such as confidentiality, privacy, and usability. Different approaches were stressed for every group in order to protect cloud data.

KEY WORDS: Cloud Computing, Security, privacy, Data-at-rest, Data-in-transit, Data-in-use

I.INTRODUCTION

Cloud Computing offers a modern method of empowering consumers with tools web-based software available. Unlike traditional approach that is based on Internet computing customers no longer, have the network entirely operated by such cloud companies, where data is processed. Computer ownership the transition of management of networks to service providers includes the adjustment of data storage obligations [1, 4, 14, 19, 31, and 34]. Information access and secrecy issues also exist. We concentrate on facets of cloud storage health and in this article.

II. SIGNIFICANCE OF THE SYSTEM

This paper reflects on topics relating to cloud security and more precisely, we are concerned with the protection of Cloud technology hosting information. When more and more information is being put on the Cloud by individuals and organizations, data protection and privacy are key concerns, especially if data are confidential, the topic of data protection and user privacy, particularly where data is sensitive is important. The study of literature survey is presented in section III, Solutions are explained in section IV, section V covers the results of the study, future study and Conclusion.

III. LITERATURE SURVEY

Cloud computing has made revolutions in IT industry through the research in service through an innovative infrastructure service delivery models for its development in real-works requirements. Approximately 90% of the users of cloud environment and computing, who are having access to their application, data and service request have a necessity of their dependencies depending on the users or customer's needs their locations, information security management, data security management, for the customers data stored in cloud virtual infrastructure environment. Data security in three dimensions: cloud characteristics, data life cycle and data security attributes

A. Classification of Data Security Issues:

For all technology, data security is a general concern. When introduced to an unregulated environment such as Cloud Computing, though, it becomes a big challenge. Distinguishing between the security threats associated with all IT infrastructures and those generated by the use of Cloud Services is significant. In general, these threats are consistent with transparent, collaborative, and distributed settings.

It is also necessary to distinguish current challenges from those posed by Cloud Computing when assessing the risks. We deal only with problems raised by the Cloud in this article, and related to results.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology

Cloud data outsourced is more insecure than stored on conventional networks, for three reasons in particular: (1) data is stored in the networks of a service provider; (2) the data of multiple users is using the same physical infrastructure; (3) data is available over the internet.
While several classifications may be created for issues of data security, we have preferred to divide them into three dimensions. Cloud characteristics, Cloud data life cycle and data security attributes. Our aim is to stress the impacts of these dimensions on data protection as well as the related common and distinct impacts on data security.

1) **Data Issues related to Cloud Characteristics:** In this segment, we are interested in data security that improves cloud-computing characteristics relative to conventional, proprietary technology. In reality, Cloud is distinct from conventional technology. These variations carry several advantages but also several inconveniences that may impact protection. The core aspects and the direct benefits and drawbacks are as follows:
Leased infrastructure:
Cloud infrastructure no longer belongs to user but to service provider. The Customer rents their use from a service supplier rather than buying unique devices. Key benefit is saving money. Main drawback is lack of influence.

Open infrastructure:
In general, cloud computing can be accessed through the Internet. Key advantage is omnipresent resources connectivity. Main drawback is different entry points.

Shared infrastructure:
Cloud infrastructure is shared by service users, unlike conventional infrastructure. Key advantage is savings in rates. Key drawback is risks of isolation failure among users.

Elastic infrastructure:
Users will scale the services up / down to meet their needs. Cloud technology then meets the current demand level, unlike conventional demand based technology. Big advantage is efficiency of resource utilization. Big drawback is assets restructuring threats.

Distributed infrastructure:
Geographically, the cloud computing is spread globally. Key benefit is improvement in computing capability and power. The biggest disadvantage is facilities administration and upkeep.
These characteristics obviously affect the data security. These capabilities have exposed the key challenges with data security.

2) **Issues of data according to the cloud data life cycle:**

Two essential resources offered by Cloud Computing [2, 5, 21] are computation and storage. Data storage is spread globally through many datacenters. Digital computers are used to analyze the results. You can build numerous virtual machines and generate numbers that match your needs [5]. They can build numbers and power. Transferring the measurement and storing of data to a third sector includes transferring their security obligations and enforcement to the third section [29].
In the cloud, the computation is performed as follows: first, the user sends his data to the processed and operated datacenter. This data is then transmitted via distributed technologies to virtual machines for parallel processing. Users can import and access the data after testing has elapsed [5]. Both personal and private data may be revealed during this process.
Based on this method, we can discern three cloud data states: data-at-rest: stored data, data-in-transit, i.e. transferred data and data-in-use; i.e. accessed or processed data. Data protection and cloud activity would also cover certain three dimensions. Different mechanisms to guarantee data protection should be set in place at either point of this data life cycle.
In this section, we illustrate problems relevant to data security in any point of this life cycle. These problems were taken from separate papers on this subject. The most important of these are overview by us:

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology

a) Data-at-rest

In this section, we address the challenges of data security at any point of this life cycle. These problems have been taken from a variety of articles on the subject. In the following data storage, we have summarized the key utilities, which are used most often in the cloud. It helps the customer to view his data omnipresent at a smaller cost than ever before. Data-at-rest refers to the storage medium protecting of data. Due to its restricted physical control over data, it is difficult for the user to accomplish. Many threats involving data storage in cloud computing are listed in the literature.

The literature discusses a variety of threats related to cloud data storage. The danger shared by most of the works has been summarized in three categories: storage media distribution risks, data localization risks, and the durability of storage media risks.

Data location risk

The first risk relates to location of physical data. The consumer data is processed at numerous locations worldwide. Cloud consumers don't necessarily know where precisely their data is stored, so it does not matter in most situations. For e.g., Face book messages and images will exist somewhere anywhere in the world and users of Face book typically have no worries. However, if an organization has confidential cloud data, it can become necessary to find the data. The cloud providers geographical locations which affect data security and privacy; in particular, data collection authorities of a nation with data residences may have access to data in compliance with the regulations of that country under some conditions[8, 14, 21, 24, 25, 28, 33].

Storage media risk

The second risk is to share physical infrastructure among numerous users. Because many users use the same physical storage space, the risk of data loss rises and affects several users. Accordingly, unwanted access by a service provider or its customers, in particular if data is confidential, is a significant issue. Theft of data, breaches, and manipulation of the data are the major dangers of sharing information [13, 14,
24, 28, 30, 31].

Storage media reliability

The third risk is the reliability of Cloud storage platform. Since users can not physically monitor data access, they must trust the vendor to protect data. In order to raise the expenses, service providers may delegate their services to another service provider without warning clients.

b) **Data-in-transit**

Protection for data-in-transit applies to data transfer protections in the cloud. It guarantees that the information is not intercepted, updated or substituted. Details in transit can be particularly confidential, such as user names and passwords. Data transmission can be more dangerous than data transmission, since you fly from one location to another [16].

c) Data-in-use

Data in use implies any reading or handling of data (created, transformed or deleted). Owing to the vast number of consumers engaging in software computing in the software, the capacity for abuse rises [22].

3) **Data Security Attributes**

Although the protection specifications vary from one data type to another (data-in-rest, data-in-transit, data-in-use). They all share a fundamental concept, which is CIA trio: Confidentiality, Integrity and Availability, but they are applied in distributed, virtual, and dynamic architecture. All security measures intended to protect one or more aspects of this trio apply these three principles. Three issues have been discussed in the majority of the literary papers [2, 4, 7, 8, 17–19, 21–23, 30, 33] on data security.

a) Confidentiality

The protection of data against unauthorized access refers to confidentiality. This is caused by outsourcing sensitive data to Cloud servers. Confidentiality is much more important in a decentralized computing context because the server hosting data is not necessarily a user's own. Cloud systems confidentiality is a major obstacle to its adoption. Currently, cloud offers are mostly public and therefore more attacks than hosting private data centers.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology

Data privacy is another confidentiality-related problem. Data Privacy concerns personal information for unauthorized persons, which must be hidden. The privacy of the user is linked to collecting, using, communicating, saving and destroying personal data. This concerns when it is not clear why personal information is used and how it is used [11].

b) Integrity

Integrity refers to data protection, whether intentional or accidental, against unauthorized changes. These changes include the creation, removal and write. In most information systems, data integrity is one of the critical elements. It can be easy to do in a centralized system but in a distributed environment like Cloud Computing, it becomes a difficult task.

The data integrity check is an important process. In general, the backup of the original data is compared with the existing data in the Cloud. The download from the Cloud, however, is a comprehensive and costly way of doing this [2]. There are currently other techniques not including the downloading of data for the integrity of data.

c) Availability

Data availability means that when authorized persons need it, information must be available. The availability of data is one of service providers' major concerns. If a Cloud service is interrupted for some reason, many customers are affected. Contractual service providers Company to ensure 99.9% performance. In addition, the collection and delivery of data and physical infrastructure in multiple areas raises the degree of availability.

There are various threats to the availability of cloud data, such as storage reliability, internet connectivity reliance, and technological defects. In general, data access is more secure in cloud than in a conventional system, so major companies like Google, Amazon, and Microsoft are better positioned than a single person or a business to handle these risks.

IV. METHODOLOGY

Solutions for data security issues:

A wide number of service models are used for cloud computing: SaaS, PaaS, and IaaS: Deployment models: private, public, community, hybrid. Therefore, the risks vary based on the cloud level used; in particular, if a private cloud protection is theoretically wide as it is monitored, the protection over a public cloud is considerably lower. Even if the user is relying on a device, network or service, the extent of control varies and the maintenance of protection can vary. IaaS offers architecture for PaaS, and provides a forum for SaaS applications creation and deployment.

In addition, cloud data can be accessible in different states, i.e., in-rest, in-use, in-transit. The data would not require the same degree of confidentiality. The processed data cannot be covered by the same means as transit or rest data.

Encryption is the main solution for the safety of the data sent and preserved. This technique is still available in Cloud today. But as with data-at - rest, this approach is not always feasible; it is also possible to actually encrypt data inside an IaaS service. Data encryption is not always possible, however, in a PaaS or SaaS program.

Cloud applications typically use data-at-rest to be unencrypted since encryption avoids scanning and indexing data. This is the case for data in use and is needed for several requests in a simple form [5, 7, 18, and 25]. IBM announced in 2009 the development of full homomorphic encryption that enables the processing of data without decryption by applications. His expense and machine sophistication are the biggest downside to this strategy.

With respect to data-in-transit, encryption is not enough to protect the form of data alone; encryption, indeed, protects confidentiality, not integrity [18]. Encryption algorithms are thus normally related to encryption and network security protocols [5, 14, 18, 22]. In comparison, the data-at-rest and data-in-transit encryption methods can be distinct. For instance, transit data encryption keys can be short-lived while data-at-rest keys can be held for a lengthy period [31].

Data security strategies otherwise rely on other factors such as the size of data and the form of data. Indeed, traditional methods for the protection of a limited amount of records, such as encryption and anonymization, may not be sufficient for large numbers. As regards data form for example, sensitive data need secrecy, while personal data need secrecy. The content of data, which is normally done using encryption methods, needs to be secured in sensitive data.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology

The user identities generally achieved through anonymising techniques are the information to be secured in the personal data. More or less availability and integrity is required for all data forms.

Our goal is to highlight the relationship between various classifications and the effect of protection on one another. We may infer that cloud technologies influence data-at-rest, data-in-use, and data-in-transit. This impact may affect their confidentiality, integrity, as well as availability. We concentrate only on the most commonly used and proven solutions.

We have classified the common security techniques according to data security attributes. The most important ones, the fundamental methods, were taken out of numerous works on literature and outlined [2, 3, 6, 8, 12, 20].
These approaches are also merged and modified to form other versions, primarily using basic encryption (symmetric or asymmetrical) to fulfill the security requirements.

Trust and legal issues are other big cloud problems. Trust is one of the best things to attain. It is difficult for the users to leave data to any third party, especially if the data are sensitive [8, 15, 19]. In the absence of confidence, security initiatives seem to be inadequate. Trust can be improved through protection regulation, accountability for suppliers and incorporation into an entity by reputable third parties, but the physical system is still under the jurisdiction of the provider even though the facilities are regulated and operated by designated persons. Users typically trust their vendors to guarantee their data security and availability, while their confidentiality and privacy are more reticent.
Legal issues include confidentiality / privacy laws and legislation in countries where data centers holding data are based [5, 8, 10, 14, 21, 24, and 31]. Since the Cloud is an evolving area, there is a lack of consensus on data protection and privacy [3]. Privacy laws and regulations are outdated and no longer extend to this modern system of data collection and processing by third parties , particularly where data is sensitive[26, 32].

V. CONCLUSION AND FUTURE WORK

Cloud Computing provides a range of advantages relative to traditional infrastructure Today, it is no longer necessary to understand what Cloud provides to the customer, but rather to understand the problem of data security that is managed by a third party. This paper addresses the problem of data security in cloud computing. First, we define data protection concerns in three dimensions: cloud characteristics, data life cycle, and data security attributes. We then defined the typical solutions used to protect data for each group of this classification.

In our classification, data security issues appear to depend on several criteria, such as data size (small / large) data type and identification (personal / private / use) and data status(used, stored or transferred). The parameters depend on individual Cloud capabilities that depend on the type / service used in their turns. The privacy, integrity, and accessible data may be influenced by these characteristics.

We have also found that the standard solutions used to securing data in the cloud system are classic methods for data securing in conventional environments such as encryption and access control. These solutions are also mixed and/or cloud-friendly.

It is also focused on the trust the customer has in the vendor, as well as legal concerns, to maintain data protection in cloud not to be summarized as a technological security solution. Protection and control of IP rights is an essential concern. Cloud Computing data transfer, collection, and analysis involve the detection of intellectual property rights defensive mechanisms for these data.

REFERENCES

1. An, Y.Z., Zaaba, Z.F., Samsudin, N.F.: Reviews on security issues and challenges in cloud computing. In: IOP Conference Series: Materials Science and Engineering, vol. 160, p. 012106. IOP Publishing (2016)
2. Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing. In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5. IEEE (2016)
3. Balogh, Z., Turčáni, M.: Modeling of data security in cloud computing. In: IEEE Annual Systems Conference, pp. 1–6. IEEE (2016)
4. Bhabad, A.V., Heda, J.R., Dhatrak, V.N., Shahane, G.P., Shirole, B.S: Data confidentiality and security in Cloud Computing using KIST algorithm. Int. J. Emerg. Trends Sci. Technol. 1 (2016). 2456-0006
5. Cercle Numérique des Industries Stratégiques (2012). http://cnis.afnet.fr/commissions/ juridique/ commission-juridique-nb02-aspects-juridiques-du-Cloud-Computing/commissionjuridique-aspects-juridiques-du-Cloud-Computing

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

6. Charanya, R., Aramudhan, M.: Survey on access control issues in cloud computing. In: IEEE International Conference on Emerging Trends in Engineering, Technology and Science, pp. 1–4. IEEE (2016)
7. Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In: IEEE International Conference on Computer Science and Electronics Engineering, vol. 1, pp. 647–651. IEEE (2012)
8. Choubey, S.D., Namdeo, M.K.: Study of data security and privacy preserving solutions in cloud computing. In: IEEE International Conference on Green Computing and Internet of Things, pp. 1101–1106. IEEE (2015)
9. Cyril, B.R., Kumar, S.B.R.: Cloud computing data security issues, challenges, architecture and methods-a survey. Int. J. Eng. Technol. 2, 848–857 (2015)
10. Delettre, C., Boudaoud, K., Riveill, M.: Cloud computing, security and data concealment. In: IEEE Symposium on Computers and Communications, pp. 424–431. IEEE (2011)
11. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4, 5 (2013)
12. Jain, P., Gyanchandani, M., Khare, N.: Big data privacy: a technological perspective and review. J. Big Data 3, 25 (2016)
13. Kulkarni, G., Gambhi, J., Patil, T., Dongare, A.: A security aspects in cloud computing. In: IEEE 3rd International Conference on Software Engineering and Service Science, pp. 547– 550. IEEE (2012)
14. Albugmi, A.A., Alassafi, M.O., Walters, R., Wills, G.: Data security in cloud computing. In: IEEE Fifth International Conference on Future Generation Communication Technologies, pp. 55–59. IEEE (2016)
15. Lenka, S.R., Nayak, B.: Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int. J. Comput. Sci. Trends Technol. 2 (2014). 2347-8578
16. Mahmood, Z.: Data location and security issues in cloud computing. In: IEEE International Conference on Emerging Intelligent Data and Web Technologies, pp. 49–54. IEEE (2011)
17. Meng, D.: Data security in cloud computing. In: IEEE International Conference on Computer Science & Education, pp. 810–813. IEEE (2013)
18. Mohamed, E.M., Abdelkader, H.S., El-Etriby, S.: Enhanced data security model for cloud computing. In: IEEE 8th International Conference on Informatics and Systems, p. CC-12. IEEE (2012)
19. Munier, M., Lalanne, V., Ardoy, P.Y., Ricarde, M.: Métadonnées et aspects juridiques: vie privée vs sécurité de l'information. In: 9ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information, pp. 65–76. SARSSI (2014)
20. Namasudra, S., Roy, P.: Secure and efficient data access control in cloud computing environment: a survey. J. Multiagent Grid Syst. 12, 69–90 (2016)
21. Priya Lyer, K.B., Manisha, R., Subhashree, R., Vedhavalli, K.: Analysis of data security in cloud computing. In: IEEE International Conference on Communication and Bio-Informatics Advances in Electrical, Electronics, Information, pp. 540–543. IEEE (2016)
22. Roy, N., Jain, R.: Cloud computing: architecture and concept of virtualization. J. Sci. Technol. Manag. 4 (2015). 2394-1537
23. Sathyanarayana, T.V., Sheela, L.M.I.: Data security in cloud computing. In: IEEE International Conference on Green Computing, Communication, and Conservation of Energy, pp. 822–827. IEEE (2013)
24. Schmitt, M.: Architecture de sécurité pour les données dans un contexte d'informatique ennuage. University of Quebec in Montreal, Master's thesis of Computer Science (2014)
25. Shaikh, R., Sasikumar, M.: Data classification for achieving security in cloud computing. Proc. Comput. Sci. 45, 493–498 (2015)
26. Shariati, S.M., Ahmadzadegan, M.H.: Challenges and security issues in cloud computing from two perspectives: data security and privacy protection. In: IEEE 2nd International Conference on Knowledge-Based Engineering and Innovation, pp. 1078–1082. IEEE (2015)
27. Shuijing, H.: Data security: the challenges of cloud computing. In: IEEE Sixth International Conference on Measuring Technology and Mechatronics Automation, pp. 203–206. IEEE (2014)
28. Singh, S., Jeong, Y.S., Park, J.H.: A survey on cloud computing security: issues, threats, and solutions. J. Netw. Comput. Appl. 75, 200–222 (2016)
29. Singh, V.K., Singh, T.: Present data security issues and their resolving technique in cloud computing. Int. J. Sci. Technol. 1, 1–6 (2016)
30. Sinha, N., Khreisat, L.: Cloud computing security, data, and performance issues. In: IEEE 23rd Wireless and Optical Communication Conference, pp. 1–6. IEEE (2014)
31. Tchifilionova, V.: Security and privacy implications of cloud computing-lost in the cloud. In: Springer Open Research Problems in Network Security, pp. 149–158. Springer, Heidelberg (2011)
32. Yu, C., Yang, L., Liu, Y., Luo, X.: Research on data security issues of cloud computing. In: IET International Conference on Cyberspace Technology, pp. 1–6. IET (2014)
33. Yu, H., Powell, N., Stembridge, D., Yuan, X.: Cloud computing and security challenges. In: ACM Proceedings of the 50th Annual Southeast Regional Conference, pp. 298–302. ACM (2012)
34. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Int. J. Internet Serv. Appl. 1, 7–18 (2010)

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

AUTHOR'S BIOGRAPHY

Prof. Dr Thirumala Rao is currently working with KL University as Assoicate Dean- Academic Registrations & Certificate courses at Vijayawada. He is also Professor in the Department of Computer Science and Engineering. He has received his Bachelors degree in Computer Science and Engineering from Nagarjuna University, Andhara Pradesh, India and Masters in Comuter Science & Engineering from JNTU, Hyderabad and PhD in Computer Science & Engineering from Acharya Nagarjuna Unviersity. He has more than 17 years of Industry,Teaching and Research experience. He has 50+ international publications in indexed journals and conferences. He is also reviewer for reputed SCI indexed journals such as Journal of Information Technology, International Journal of Cloud Computing of Inderscience Publishers. He is also active member of professional societies such as ACM,IEEE etc…and chaired several Springer, IEEE international conferences. His research interests include Cloud computing, Big Data Analytics, IoT based systems and use cases.