ISSN No:-2456-2165

Data Security in Cloud Computing

Zeel B Dabhi
MCA DS
School of Engineering
Ajeenkya DY Patil University
Pune (MH) 412105

Akanksha Kulkarni
Ajeenkya DY Patil University
Pune(MH) 412105

Abstract:- The importance of data security has been a significant problem in information technology. Because the data is spread out all over the place in the field of technology, it becomes extremely problematic. Users' primary worries regarding cloud computing are related to data security and privacy security. Despite the fact that numerous approaches to the issue of cloud computing have been studied in academic research and clinical trials, data security and privacy protection are becoming increasingly crucial for the future use of cloud computing technology in business, industry, and government. In the cloud architecture, concerns about data security and privacy security apply to both hardware and software. This research aims to improve data security and privacy security for a reliable cloud environment by examining various security strategies and exceptions from both software and hardware aspects for securing data in the cloud. a comparison of the study that has already been done on the data security and privacy security methods utilised in cloud computing.

Keywords:- *Cloud Computing, Data Security, Privacy, and Data Protection.*

I. INTRODUCTION

In Simple Terms, It means storing, managing and accesing the data and program on the remote servers that are hosted on internet instead of computers hard drive [1].

For example, Google Cloud, AWS (Amazon Web Service), IBM Cloud, etc.

- *Characteristics of cloud computing:-*

1. On-Demand Self-Service: A customer can request and obtain access to a service without the need for a manual response from an administrator or other support staff.
2. Bread network access:- The service can be accessed from any location.
e.g. any where access & anytime.
3. Resourse pooling:- Resource can be storage, memory, virtual machine. computing has been envisioned as the upcoming generation paradigm in computation surrounding, both Applications and resources are made available as services through the Internet. It can be any servers which can be consumed by cloud users. Resource pooling means that multiple customers are server from the some physical resources.
4. Meaured services:-Pay according to the servers you use.
5. Rapid easily The ability to instantly deploy resources in the cloud as needed by the company (and remove them when they are no longer needed) is one of the best aspects of cloud computing.
6. No maintenance /easy maintenance
7. Security:- copy of over data on various service. If one fails, data is secure on the other.

Cloud data security is a technological mix. solutions, policies, and procedures that you implement. to protect cloud-based applications and systems, along with the associated data and user access. resources for hardware and software in data centres that provide a variety of services across a network or the Internet to satisfy user's demand [2].

The simplify of **cloud computing** from the National NIST is the National Institute of Standards and Technology, A shared pool of reconfigurable computing resources (such as networks, servers, storage, etc.) that can be instantly deployed and released with minimum administration effort or service provider involvement is made possible by cloud computing. Cloud computing offers quick on-demand network access to a pool of adjustable resources that are shared. computing assets. Assets turn to computing applications, network assets, platforms, software services, virtual servers, and computing infrastructure.

Cloud computing is very optimistic for the IT applications; however, there are still some complication to be solved enabling individuals and businesses to store data and find applications in the cloud computing environment. Data security is one of the most crucial boundaries to establish and is governed by problems like permission, privacy, trust, and legal considerations. a portion of institutions and institutional development is close to privacy and security when using the cloud.

Data security has always been a big problem in IT. Because data are stored separately on servers, PCs, and a variety of mobile devices including wireless sensor networks and smartphones, data security becomes a top priority in the cloud computing environment. Compared to on-premises security, cloud computing data security requires more work. established information systems. The specific controls and technologies used to enforce.

Information governance. They are classified below:

Detecting and preventing data migrations to the cloud include to the internal data migration and movement to the cloud and second is protecting data moving to the cloud include to the application/client encryption both proxy-based encryption and link/network encryption. Keeping cloud data secure is content discovery, laaS Encryption, PaaS encryption, saaS encryption.

Cloud computing immaterial provides two basic types of functions: computing and data storage. data storage, data keep safe and security are the primary factors for acquire user's trust and making the cloud technology successfully used. A number of data protect and data security techniques have been put forward in the research field of using the cloud.

In this section, we'll examine several security measures and issues related to protecting users' privacy and data storage in the cloud computing environment. The facility employed in cloud computing is discussed in this study in relation to previous research work on data security issues, including data integrity, privacy, and availability. Because data privacy generally goes hand in hand with data security, cloud technologies and data privacy problems are also investigated. By protecting data in the cloud computing sector, relevant research on data security and privacy may assist to increase the user's confidence.

II. DATA INTEGRITY

One of the most important components of any information system is data integrity. Data integrity is the absence of unauthorised data production, modification, or deletion. With a single database, data integrity may be readily accomplished in a unique system. Database constraints and transactions, which a database management system normally completes, ensure data integrity in one system (DBMS). Transactions should follow the ACID (atomicity, consistency, isolation, and durability) requirements to ensure data integrity. Most databases are capable of handling ACID transactions and maintaining data integrity. control the access to data in accordance with utilised. It is the method through which a system decides how much access a specific authorised user should have to its secure resources. In a cloud system, preserving data integrity entails information integrity protection. The data shouldn't be lost or changed by unauthorised users. Data integrity is the cornerstone for providing cloud computing services like SaaS, PaaS, and IaaS. Therefore, cloud computing environments typically offer data processing services for large-scale data storage. Data integrity can be offered through techniques like digital signatures and RAID-like systems. The prerequisite for deploying applications is to remotely check the accuracy of data in the cloud. Growth et al By integrating error detection and remote data integrity checking correcting code with spot-checking, the theoretical framework "Proofs of Retrievability" was presented. The HAIL system employs the POR mechanism to investigate how data is kept in various clouds.

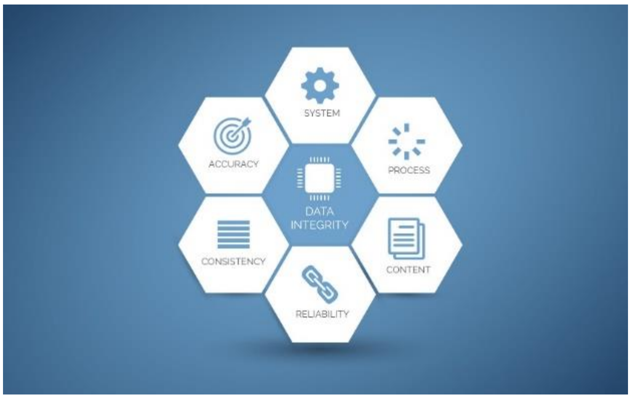


Fig 1 Data Integrity

III. DATA CONFIDENTIALITY

Data access is reportedly controlled by usage. The method through which users save their personal data in the cloud is crucial for maintaining confidentiality of data. Access control and authentication methods are used to ensure information security. The issues with data confidentiality, authentication, and access control in cloud computing could be remedied by improving cloud reliability and trustworthiness. Information is most valuable asset you posses.

Proprietary information means about ownership and handle with equal care. confidential information is access/distribution is restricted.

Access/distribution rights is who, what, where, when, how. Confidentiality levels Is most important part in data confidentiality.

Confidentiality levels is electronic documents, fast to create/distribute. Preface with "CONFIDENTIAL".

Practical confidentiality restrictions is only use it for its stated purpose. Only disclose it to parties with its stated purpose. Delete it upon request or after its stated purpose.

You must know its propose and affiliated parties. Preface with "CONFIDENTIAL TO CEO, CFO, …."

One is homomorphic encryption. Encryption is frequently used to safeguard the confidentiality of data. Homomorphic encryption was recommended as a sort of encryption scheme by Rivest et al.

An encrypted database and search. Researchers are currently concentrating on the applications of the limited homomorphic encryption algorithm in the cloud environment due to the inefficiency of the homomorphic encryption technique. A frequent procedure is encrypted search.

Fig 2 Data Confidentiality

A. *Distributive Storage.*

A potential strategy in the cloud context is distributed data storage. AlZain et al. highlighted issues with data privacy security, as well as data integrity, infiltration, and service availability in the cloud. Storing data across many clouds or cloud databases is one way to ensure data integrity. According to the designed active measurement, Arfeen et al. describe how cloud computing resources are distributed. The system architecture, the unique pathways for incoming and outgoing traffic, and progressively adjusting the resource allocation in accordance with user demands form the foundation of the personalised measuring approach.

B. *Hybrid Method.*

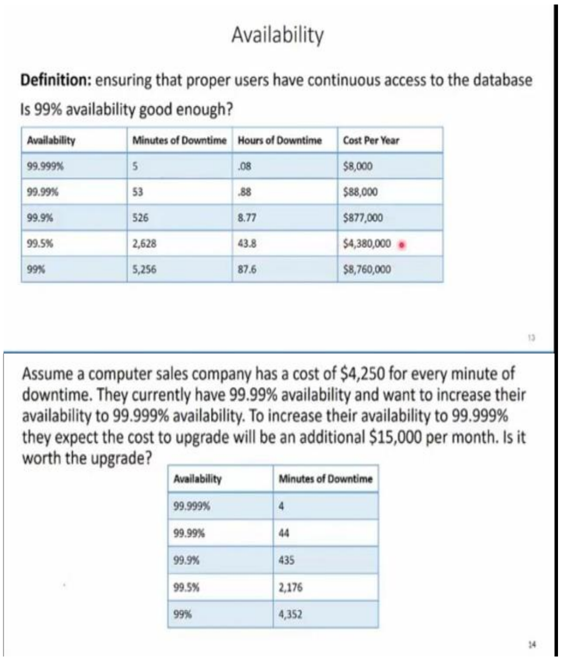
For data security and integrity, a hybrid methodology is put forth that makes use of both key sharing and authentication methods. The connection between the user and the cloud service provider may be made more secure by using robust key sharing and authentication methods.

IV. DATA AVAILABILITY

Data accessibility translates to: How much of a user's data can be utilised or retrieved in the event of an accident, such as a network outage, IDC fire, or hard disc damage, as well as how customers may independently check their data rather than just relying on the cloud service provider's credit guarantee. Due to the fact that cloud suppliers are subject to local regulations and as a result, cloud customers, the problem of data storage across international servers is one that the clients take very seriously. should be cognizant of those laws.

Users' faith in the cloud may be increased by finding data. Users can access transparent storage through cloud storage, which can reduce cloud complexity but also limit users' ability to manage their data storage. Benson et al. analysed the geographic replication proofs and were successful in identifying the Amazon cloud data.

- *Data availability example:-*



Availability

Definition: ensuring that proper users have continuous access to the database

Is 99% availability good enough?

Availability	Minutes of Downtime	Hours of Downtime	Cost Per Year
99.999%	5	.08	$8,000
99.99%	53	.88	$88,000
99.9%	526	8.77	$877,000
99.5%	2,628	43.8	$4,380,000
99%	5,256	87.6	$8,760,000

13

Assume a computer sales company has a cost of $4,250 for every minute of downtime. They currently have 99.99% availability and want to increase their availability to 99.999% availability. To increase their availability to 99.999% they expect the cost to upgrade will be an additional $15,000 per month. Is it worth the upgrade?

Availability	Minutes of Downtime
99.999%	4
99.99%	44
99.9%	435
99.5%	2,176
99%	4,352

14

Fig.3 Data Availability Example

Dependable storage contract Some of the user's update data may be deleted by the cloud service providers, which is a frequent anomalous behaviour of untrusted storage and difficult to monitor only depending on the simple data encryption. A good storage agreement must also let numerous users to modify data simultaneously. Mahajan et al. suggested Depot that can provide eventual consistency and fork-join causal consistency. It can assist the adoption of other safety precautions in the trusted cloud storage environment and successfully fend against assaults like discarding.

Feldman et al. proposed SPORC, which can implement the safe and reliable real-time interaction and collaboration for multiple users with the help of the trusted cloud environment, and untrusted cloud servers can only access the encrypted data.

V. DATA AVAILABILITY AS PART OF DATA MANAGEMENT

Different businesses have different levels of time sensitivity. Every firm wants their data to be as accessible as possible, but those that have a pressing need to restore data availability immediately may need to make a sizable investment in a system that can meet their requirements.

Data availability issues should not be considered resolved in a data management plan until they have been fully handled.

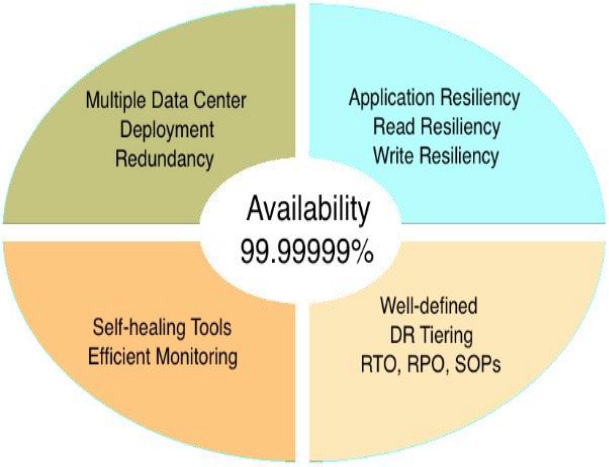


Fig.4 Data Availability Graph

- *Reliability of Hard-Drive.*

Currently, the primary storage medium in a cloud environment is a hard disc. Hard disc dependability creates the framework for cloud storage. Pinheiro et al. analysed the hard disc error rate using hard drive history data.

VI. DATA PRIVACY

The use of data privacy in cloud computing enables the collection, archiving, transmission, and sharing of data via the internet without jeopardising the private of specific users' personal data. Customers usually are unaware of how the processing of their cloud-stored personal data takes place. With the popularity of the cloud growing, data privacy is turning into a crucial aspect of cloud computing.

By data privacy, we imply that no one else is viewing or sharing your sensitive information that you post online. You may exchange data while maintaining the privacy of your personal information.

Connect cloud computing with data privacy right now. With the cloud's rising popularity, millions of people are storing their personal, business, or both types of data online. Many cloud users aren't even aware of the precise location of the server hosting their data or the methods used to analyse it. those computers.

Privacy has the following elements. When: Rather than worrying about past facts coming to light, a person may be more concerned about facts from the present or the future. (ii) How: While a user could feel comfortable if their friends individually ask them for information, they might not like getting regular and automated messages. (iii) Extent :A user may choose that their information be reported as a general area rather than a specific area specific location.

Fig 5 Data Privacy

VII. CONCLUSION

The newest and most promising technology for the next wave of IT applications is cloud technology. The analysis of data and information is always the most important activity in all businesses, and any company must lower the cost of data processing and storage. for making decisions. Therefore, until clients and cloud service providers can build trust with one another, no business will migrate its data or information to the cloud. More work needs to be done in the field of cloud computing to win over users of cloud services. This study focused on how data is stored and used in the cloud for data protection in cloud computing settings, looking at various data security and privacy solutions. to increase consumer and cloud service provider trust.

ACKNOWLEDGMENT

Prof. Akanksha Kulkarni of ADYPU has my sincere gratitude for her insightful and helpful advice throughout the inception and progress of this research project.

REFERENCES

[1]. R. Latif, H. Abbas, S. Assar, and Q. Ali, “Cloud computing risk assessment: a systematic literature review,” in Future Information Technology, pp. 285–295, Springer, Berlin, Germany, 2014.

[2]. A. Avizienis, J. Laprie, B. Randell, and C. Landwehr, “Basic ˇ concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[3]. Z. Mahmood, “Data location and security issues in cloud computing,” in Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT ’11), pp. 49–54, IEEE, September 2011.

[4]. D. Sun, G. Chang, L. Sun, and X. Wang, “Surveying and analyzing security, privacy and trust issues in cloud computing environments,” in Proceedings of the International Conference on Advanced in Control

Engineering and Information Science (CEIS ’11), pp. 2852–2856, chn, August 2011.

[5]. A. Pandey, R. M. Tugnayat, and A. K. Tiwari, “Data Security Framework for Cloud Computing Networks,” International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178–181, 2013.

[6]. D. A. Klein, “Data security for digital data storage,” U.S. Patent Application 14/022,095, 2013.

[7]. M. Y. A. Younis and K. Kifayat, “Secure cloud computing for critical infrastructure: a survey,” Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

[8]. S. Kardas¸, S. C¸ elik, M. A. Bingol, and A. Levi, “A new security ¨ and privacy framework for RFID in cloud computing,” in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol , UK, 2013.

[9]. A. Behl, “Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation,” in Proceedings of the World Congress on Information and Communication Technologies (WICT ’11), pp. 217–222, IEEE, December 2011.

[10]. D. Chen and H. Zhao, “Data security and privacy protection issues in cloud computing,” in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651, Hangzhou, China, March 2012.

[11]. K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: theory and implementation,” in Proceedings of the ACM Workshop on Cloud Computing Security (CCSW ’09), pp. 43–53, November 2009.

[12]. K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” in Proceedings of the 16th ACM conference on Computer and Communications Security, pp. 187–198, ACM, Chicago, Ill, USA, November 2009.

[13]. J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, “Seeding clouds with trust anchors,” in Proceedings of the ACM workshop on Cloud computing security workshop (CCSW ’10), pp. 43–46, ACM, October 2010.

[14]. D. H. Rakesh, R. R. Bhavsar, and A. S. Thorve, “Data security over cloud,” International Journal of Computer Applications, no. 5, pp. 11–14, 2012.

[15]. R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.

[16]. C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009

[17]. N. Leavitt, “Is cloud computing really ready for prime time?” Computer, vol. 42, no. 1, pp. 15–25, 2009.

[18]. P. Mell and T. Grance, “The nist definition of cloud computing,” National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.

[19]. F. Berman, G. Fox, and A. J. G. Hey,Grid Computing: Making the Global Infrastructure a Reality, Volume 2, John Wiley and sons, 2003.

[20]. M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” IACR Cryptology EPrint Archive, vol. 186, 2008.

[21]. Z. Xiao and Y. Xiao, “Security and privacy in cloud computing,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, 2013.

[22]. N. Kshetri, “Privacy and security issues in cloud computing: the role of institutions and institutional evolution,” Telecommunications Policy, vol. 37, no. 4-5, pp. 372–386.

[23]. P. Mahajan, S. Setty, S. Lee et al., “Depot: cloud storage with minimal trust,”ACM Transactions on Computer Systems, vol. 29, no. 4, article 12, 2011.

[24]. A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, “SPORC: group collaboration using untrusted cloud resources,” in Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI ’10), vol. 10, pp. 337– 350, 2010.

[25]. E. Pinheiro, W.-D. Weber, and L. A. Barroso, “Failure trends in a large disk drive population,” in Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07), vol. 7, pp. 17–23.