Survey Paper on Critical Section & Privacy Issue in Cloud Computing

[1]Neha M. Sarade, [2]Meet Poladia, [3]Dheeraj Pandey
[1,2,3] PG Students
[1]Department of Computer Engineering, [2,3]Department of Electronics & Telecommunication Engineering.
Sardar Patel Institute of Technology, Mumbai, India.

***Abstract* - In the cloud computing environment, data security has consistently been a major issue and it becomes particularly serious because the data is located in different places even in all the world. Data security and privacy protection are the two main factors of user's concerns about the cloud. In this paper, we make a comparative research analysis of the existing research work with reference to the data security and privacy protection techniques used in the cloud computing.**

***Index Terms* - Cloud; cloud computing; service provider; data storage; data security; data correctness; data availability; data integrity.**

I. Introduction

A This Cloud computing has been visualized as the next generation model in computation. In the cloud computing environment, both applications and resources are handed over on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide several services over the network or the Internet to satisfy user's requirements [1].

The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST) [2] is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the explanation, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure.

The three well-known and commonly used service models in the cloud model are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider forward services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business efficiency.

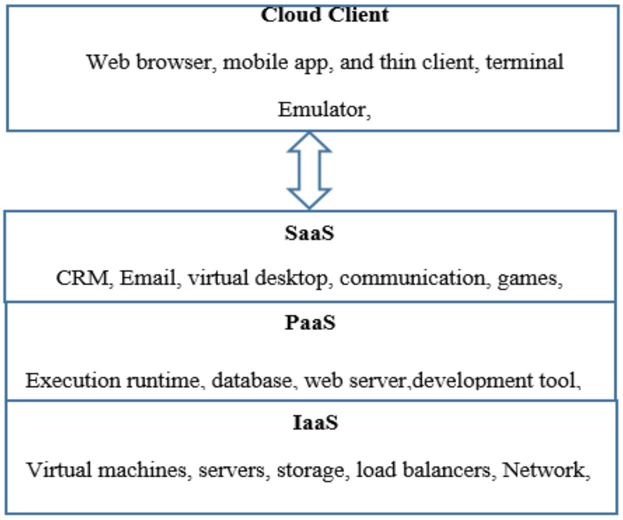
Cloud Client
Web browser, mobile app, and thin client, terminal Emulator,
SaaS
CRM, Email, virtual desktop, communication, games,
PaaS
Execution runtime, database, web server,development tool,
IaaS
Virtual machines, servers, storage, load balancers, Network,

Fig 1: Conceptual cloud architecture

II. Literature Survey

In this paper, we will review different security techniques and challenges for data storage security and privacy protection in the cloud computing environment.

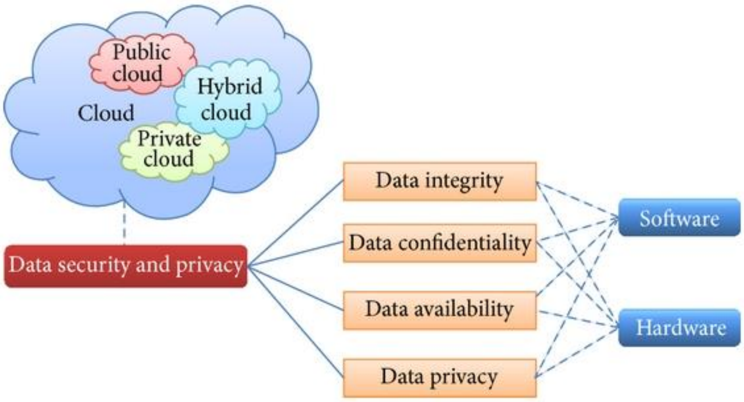

Fig 2. Organization of data security and privacy in cloud computing.

As shown in Fig.2, a comparative research analysis of the existing research work regarding the techniques used in the cloud computing through data security aspects including data integrity, confidentiality, and availability.

Data privacy issues and technologies in the cloud are also studied, because data privacy is traditionally associate with data security.

1. Data Integrity

Data integrity means protecting data from unauthorized modification, deletion, or falsification..The data should not be lost or modified by unauthorized users. Along with data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Verifying the integrity of data in the cloud remotely is the reward to deploy applications. Bowers et al. proposed a theoretical framework "Proofs of Retrievability" to realize the remote data integrity checking by combining error correction code and spot-checking [3]. The HAIL system makes the uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking.it also describe that how HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers [4]. Schiffmanet al. proposed trusted platform module (TPM) remote checking to check the data integrity remotely [5].

To ensure the data integrity, one option could be to store data in multiple clouds. The data to be protected from internal or external unauthorized access are divided into chunks and Shamir's secret algorithm is used to generate a polynomial function against each chunk. Ram and Sreenivaasan [11] have proposed a technique known as security as a service for securing cloud data. The proposed technique can achieve maximum security by dividing the user's data into pieces. These data chunks are then encrypted and stored in separated databases as each segment of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks.

2. Data Confidentiality

Data confidentiality is necessary for users to store their private or confidential data in the cloud. Access control strategies and authentication are used to provide data confidentiality

- Homomorphic Encryption

Encryption is usually used to ensure the confidentiality of data. Homomorphic encryption is a type of encryption system proposed by Rivest et al. [6]. It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results; besides, the whole process does not need to decrypt the data. The implementation of this technique could well solve the confidentiality of data and data operations in the cloud.

A cryptographic algorithm named Diffie-Hellman is proposed for secure communication [7], which is absolutely dissimilar to the key distribution management mechanism. For more flexibleness and enhanced security, a hybrid technique that merge multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed [8]. RSA is useful for establishing secure communication connection through digital signature based authentication while 3DES is particularly useful for encryption of block data. Besides, several encryption algorithms for ensuring the security of user data in the cloud computing are discussed [9].

- Hybrid Technique

A hybrid technique is designed for data confidentiality and integrity [12], which uses both key sharing and authentication techniques. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA is an asymmetric cryptographic and public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

A three-layered data security technique is introduced [13] the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring privacy and protection; and the third layer does fast recovery of data by a speedy decryption process.

An event-based isolation of critical data in the cloud approach is proposed [14], Trust Draw, a transparent security extension for the cloud which combines virtual machine introspection (VMI) and trusted computing (TC).

3. Data availability

Data availability means the when accidents such as network failures ,IDC fire and hard disk damage occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the guarantee by the cloud service provider alone. Benson et al. studied the proofs of geographic replication and achieve a success in locating the data stored in Amazon cloud [14].

- Reliable Storage Agreement

The most abnormal behavior of untrusted storage is that the cloud service providers may discard part of the user's update data, which is difficult to be checked by only lean on the simple data encryption. Also, a good storage agreement needs to support parallel modification by multiple users. Feldman et al. proposed SPORC [15], which can implement the safe and reliable real-time communication and collaboration for multiple users with the help of the trusted cloud environment, and un trusted cloud servers can only access the encrypted data.

4. Data Privacy

The privacy issues differ according to different cloud scenarios and can be divided into four subcategories [16,17,18] as follows:

(i) How to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, malicious use, and unauthorized resale,

(ii) How to guarantee data replications in a administration and consistent state, where replicating user data to multiple suitable locations is an prevailing choice, and avoid data loss, leakage, and unauthorized modification or falsification.

(iii) Which party is responsible for ensuring legal requirements for personal information?

(iv) To what extent cloud subcontractors are involved in processing which can be properly identified, checked, and verify.

Summon Cherian, Kavitha Murukezhan[19] defined the idea to provide Data Protection as a Service in Cloud Computing,.There are basically two types of keys they are public key and private key. A public key is known to everyone and a private or secret key known only to the recipient of the message. An authorized user has the key for encryption and decryption of the specific data file. Keyword based search is one of the popular ways to collectively identify and retrieve data files instead of retrieving all the files. Keywords are parts of file name or phrases used in the file which will help us to find the exact data file at the time of retrieval if you don't remember the exact keyword. There are many keyword searching methods.

Rakhi Bhardwaj et al. [20] have described dynamic data auditing policy for the data storage on the cloud. They have discussed an auditing model for the data storage in cloud which consists of data owner auditing, Third Party Auditing (TPA) and derived the resulting research where TPA can support the dynamic auditing for multiple tasks simultaneously. Thus, the high performance on data availability and integrity can be achieved

In [21], Kalpana Batra et al. have tried to achieve the security of data in distributed storage system by applying the file distribution technic to provide the redundancy. For correctness of the data they have generated the token pre computation technic and stored at servers in cloud for the verification purpose. They have shown that their scheme is efficient and reliable to detect the misbehaving servers and correct the data in particular servers and avoid colluding attacks of server modification by unauthorized users

Table –I Critical Evaluation of Security and Privacy in Cloud Computing

Ref	Research Topic	Issues Mentioned	Solution Proposed	Benefits
W.A Jansen [22]	Security and Privacy issues in Cloud Computing	Trusted and reliable computing	Service Level Agreements, Policies and Procedures, Risk Management.	Data Security and Privacy will be ensured
K. Julisch and M. Hall [23]	Security and Control in Cloud Computing	Security and controls concerns	Service Level Agreements, Virtual Information, Security Management System (ISMS).	Standard compliant management process and assets protection will be ensured
D. Mohammed [24]	Secure Cloud Computing	Social and Technological Constraints	Proposed a solution to address Compliance, Transparency, Encryption and Multi-tenancy.	Data privacy will be ensured

Z. Mehmood [25]	Security and Data Storage Location in Cloud Computing	Data issues of storage location, cost, availability and security	Appropriate use of cloud technologies.	Data storage location and availability will be ensured
D. Svantesson and R. Clarke [26]	Risk in Cloud Computing	Legal Regulatory Aspects and Consumer Rights	Improvement in consumer rights and privacy laws.	Consumer rights protection will be ensured
D. H. Patil, R. R. Bhavsar and A. S. Thorve [27]	Data Security in Cloud Computing	Data Access Control	A solution to address authentication mechanism.	Security, privacy and compliance will be ensured
D. Chen and H. Zhao [28]	Security Controls in Cloud Computing	Life Cycle Data on Cloud	Data Security and Privacy.	Data Identification, Isolation and Privacy protection will be ensured
B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit [29]	Service Level Agreements for Secure Cloud	Client Compliance and Trust	Compliance, Trust, Data Segregation and Recovery.	Data security policies and procedures will be ensured

CONCLUSION

Cloud computing is a encouraging and emerging technology for the next generation of IT applications. The hurdle toward the rapid growth of cloud computing are data security and privacy issues. In all the organizations for decision making reducing data storage and processing cost is a mandatory requirement , while analysis of data and information is always the most important tasks. So no organizations will transfer their data or information to the cloud as far as the trust is created between the cloud service providers and customer. A number of approaches have been suggested by researchers for data protection and to obtain more data security in the cloud. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments.

REFERENCES

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

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

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

[4] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” inProceedings of the 16th ACM conference on Computer and Communications Security, pp. 187–198, ACM, Chicago, Ill, USA, November 2009.M. Young, The Technical Writer's Handbook. Mill Valley, CA: UniversityScience 1989.

[5] 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

[6] 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..

[7] D. Boneh, “The decision Diffie-Hellman problem,” in Algorithmic Number Theory, vol. 1423, pp. 48–63, Springer, 1998.

[8] A. Kaur and M. Bhardwaj, “Hybrid encryption for cloud database security,” Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012.

[9] R. Arora, A. Parashar, and C. C. I. Transforming, “Secure user data in cloud computing using encryption algorithms,” International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013.

[10] M. A. AlZain, B. Soh, and E. Pardede, “Mcdb: using multi-clouds to ensure security in cloud computing,” in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11), pp. 784–791, 2011.

[11] C. P. Ram and G. Sreenivaasan, “Security as a service (sass): securing user data by coprocessor and distributing the data,” in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[12] A. Rao, “Centralized database security in cloud,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544–549, 2012

[13] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, “Enhanced data security model for cloud computing,” in Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12), pp. CC-12–CC-17, IEEE, 2012.

[14] K. Benson, R. Dowsley, and H. Shacham, “Do you know where your cloud files are?” in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, pp. 73–82, ACM, October 2011.

[15] 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.

[16] S. Pearson and A. Benameur, “Privacy, security and trust issues arising from cloud computing,” inProceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science (CloudCom '10), pp. 693–702, IEEE, December 2010.

[17] S. Paquette, P. T. Jaeger, and S. C. Wilson, “Identifying the security risks associated with governmental use of cloud computing,” Government Information Quarterly, vol. 27, no. 3, pp. 245–253, 2010.

[18] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.

[19] Sunumol Cherian, Kavitha Murukezhan“ Providing Data Protection as a Service in Cloud Computing,” International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013 1 ISSN 2250-3153

[20] Rakhi Bhardwaj, Vikas Maral, “Dynamic Data Storage Auditing Services in Cloud Computing”, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[21] Kalpana Batra, Ch. Sunitha, Sushil Kumar,” An Effective Data Storage Security Scheme for Cloud Computing”, International Journal of Innovative Research in Computer and Communication Engineering

[22] W. A. Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing”, 44th Hawaii International Conference on System Sciences - 2011, IEEE.

[23] K. Julisch and M. Hall, “Security and Control in the Cloud”, Information Security Journal: A Global Perspective, vol. 19, **(2010)**, pp. 2099-309.

[24] D. Mohammed, “Security and Cloud Computing: An Analysis of Key Drivers and constraints”, Informatio Security Journal: A Global Perspective, vol. 20, **(2011)**, pp. 123-127.Z. Mehmood, “Data Location and Security Issues in Cloud Computing”, International Conference on Emerging Intelligent Data and Web technologies, IEEE, **(2011)**.

[25] D. Svantesson and R. Clarke, “Privacy and Consumer Risks in Cloud Computing”, Computer Law and Security Review, vol. 26, **(2010)**, pp. 391-397

[26] D. H. Patil, R. R. Bhavsar and A. S. Thorve, “Data Security over Cloud”, International Journal of Computer Applications® (IJCA), **(2012)**.

[27] D. Chen and H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, 2012 International Conference on Computer Science and Electronics Engineering, IEEE.

[28] B. R. Kandukuri, R. Paturi V and Dr. A. Rakshit, “Cloud Security Issues”, 2009 IEEE International Conference on Services Computing, IEEE.

IJEDR