Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 8, 2020

A Effective Retrieval and Task Scheduling on Cloud Data Storage

R.Prabhu[1] , Dr.S.Rajesh[2]
[1]Department of Computer Science and Engineering,
AAA College of Engineering & Technology, Amathur, Sivakasi-626 005, Tamil Nadu, India

[2] Department of Information Technology,
MepcoSchlenk Engineering College ,Sivakasi-626005, Tamil Nadu, India

Received: 11.03.2020 *Revised: 12.04.2020* *Accepted: 28.05.2020*

ABSTRACT

Cloud computing is a modern way of computing, enabling a wide range of sharing computer resources through the internet. Cloud computing is distributed in nature delivering effective on-demand services globally. According to the current real-time scenario, cloud computing is boon for the information technology paradigm that serving a higher level of data outsourcing with minimal management effort. The main key term on cloud computing is pay per use as well as data storage facilities. However, this technology had made a high impact among the organizations, but stillaverage number of firms neglecting these services with some strong reasons. The major issue in this technology is the lack of security. The organizations storing highly sensitive information on the cloud database and here data protection along with privacy is still a challenge. In this paper, we are not cover whole challenges, our work concentrated on a few severe security challenges and the techniques used to overcome these issues. It also describes those technologies merits and demerits in an effective manner. In addition in this work we analysis several tactics related to privacy protection affairs, securing sensitive data, reliability and enabling accuracy from the unauthorized users in the cloud environment.

Keywords: Cloud Computing, Security, Data Protection and On-demand services, Task SchedulingSTRACT

1. Introduction:

Cloud computing is termed as a network of services through the internet. The need for high-cost resources and other related services by the organization raises the cloud evolution rapidly. It generally works in the aspect of request and response. There are several cloud providers delivering enhanced services globally. Some of the popular cloud providers are Amazon, Google, and Dropbox. Cloud computing is popular for its enormous storage facility as well as pay per use options. Nowadays the cloud environment has improved their technology and enables central servers by which performing distributed operations over multiple locations. The cloud architecture consists of components and subcomponents. Each component is responsible for specific operations like front end platform, back end platforms, cloud-based delivery, and network services. A centralized cloud provider is responsible for taking request from the client and delivering the services as per the queue along with security. The below figure;

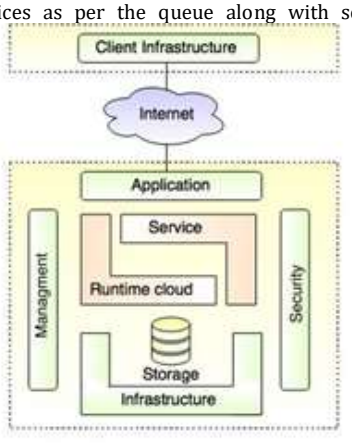


Fig 1: Cloud computing architecture

Generally, the cloud is of three types such as public, private and hybrid. Public cloud is a general cloud provider delivering cloud computing to any public cloud users. In this, there will be a huge data center providing computing hardware for their clients. Private cloud, as its name specifies these are specialized for single organizations. Most of the larger organizations use these kinds of the cloud to maintain security and reliability. Several customizations and cost options were provided on these private clouds as per the organization needs. Hybrid clouds are a combination of both public and private clouds. Hybrid cloud is similar to a multi-cloud environment providing various cloud services with the combination of public and private clouds. In the cloud environment, the service models are classified into three models such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

Characteristics of Cloud Environments:

- On-demand self-service: Enables users to sign up and pay for what they use then log out. It provides quick accessing cloud resources without any sales agents.
- Broad network access:Cloud services by means of through the internet.
- Resource pooling: Generally customers are of various kinds such as individuals, organizations and different departments within an organization. Cloud computing provides the same server, storages or other resources for them remotely.
- Rapid elasticity or expansion: Easy monitoring and scaling of their resource usages. By which they can change their resources as needed.
- Measured service: Pay per use on what the resources used according to the time period, instead of paying entire hardware or software amounts.

However cloud computing is rich with several benefits, it has some severe challenges to overcome. The enormous need for cloud computing and its growth grabs the attention of the research community. The most important issue to be overcome on cloud computing security breach and storage maintenance. The below figure describes some of the cloud computing risks still existing

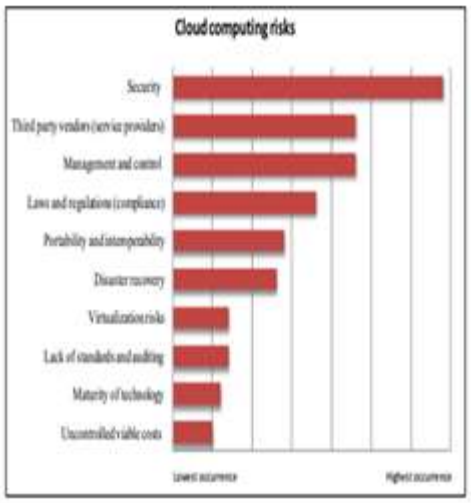
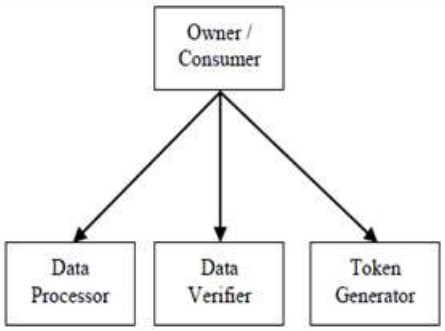


Fig 2: Cloud Computing Risks

This paper is organized as follows; section 2 describes the Cloud Storage Basics & Challenges in several aspects. In section 3 we discussed the Mobile Cloudata Storage Security and Privacy. Section 4 holds the conclusion part.

Cloud Storage Basics & Challenges:

Cloud storage is a resource which enables the user to manage their database remotely by means of a centralized server through internet. By which the authorized user can able to access, upload and download their files from anywhere anytime. According to the National Institute of Standards and Technology (NIST) [2], cloud computing is the most reliable on-demand computing utility for storing. Nowadays one of the major components in cloud computing is database outsourcing, in which by means of the service provider (cloud provider) the owner can outsource data managementknown as Database-as-a-Service (DaaS) [3]. Security and privacy are the two factors that prevent the databases from the attackers. Using the third party as a service provider enables the loss of data to some extent due to the ownership offline. For backup and secure the loss of data chunking operation is applied [4]. Chunking is the process enabling the client to create a token in the master server and stores the files in the client-server using token generation along with merging algorithms.



Wenjie Liu et al [5] presented a Quantum-Based Database Query methodology for preserving the privacy in cloud computing. In this work, the author enables the user to retrieve their information by means of privacy-preserving database queries. To maintain privacy, initially, the databases were getting encrypted and transmitted with different keys for protection. To enable this the author combines modified Grover iteration and special offset encryption mechanism to execute the correct query for processing the desired data items.

Yanwei Xu et al [6] presented a Collaborative Filtering- (CF-) technique for preserving privacy in a distributed cloud environment. In this work the author concentrated on two major issues, the first one is the decrease of cross-cloud service. This is because the cloud platform never allows sharing the details to another cloud platform because of a security breach. The second one is dealing with historical data which are outdated that minimize the cloud scalability. The author addressed these two issues by proposing SimHash, a novel privacy-preserving and scalable service scheme.

Lianyong Qi et al [7] presented a Hashing-Based method for Multi-Source Data in the cloud environment. The main intention of this work is improvising the data quality of historical user services. For a cloud platform, it is difficult to take a decision where the cloud user appeals services from various distributed cloud platforms. By means of distributed locality-sensitive hashing, first privacy is protected from multiple sources and then user quality data services are improved. The efficiency of this approach is tested by using the WS-DREAM data set.

Xu AnWang et al [8] presented encryption with fine-grained searchable capability on marinating the privacy in the cloud. In this work the author proposed Predicate Encryption method instead of traditional public key encryption. It is dual system encryption proves surety by IND-AH-CPA (indistinguishable under chosen plain-text attack for attribute-hiding). Initially, the relationship among searchable encryption and predicate encryption is well analyzed, based on that Public-Key Encryption with Fine-grained Keyword Search method is proposed. Comparing to the other traditional schemes it satisfies common security breaches in the cloud.

Bing Wang et al [9] presented an Inverted index based multi-keyword public-key searchable encryption technique. The main intention is to prevent sensitive information from the attackers. Several existing solutions have a one-time-only search limitation. The inverted index is one of the most popular searchable index structures which preserves high search competence. In the proposed scheme the author uses trapdoor generation algorithm for protecting the search patterns and also supporting the conjunctive multi-keyword search. The performance is far better than the public key based schemes.

Chintada et al., [10] presented her work by classifying the security affairs into two types such as cloud customer-based issues and cloud provider based issues. Initially, the cloud provider to secure the infrastructure, by which user's information's and applications will be safe. On the other aspect, the customer needs to satisfy that the provider's infrastructure is safe in preventing the customer's information's from the attackers.

Kaitai and Willy [11] presented a re-encryption system based on searchable attributes. This proposed scheme supports sharing the policies between the data owners to the specified data groups where the policy matched. A separate keyword is processed and updated to the users, based on that a re-encryption is done and the key is shared to the data owners privately. This scheme supports flexible keyword update services.

Bala Chandran et al., [12] presented a proposed distributed auditing mechanism for ensuring the stored data's data corrections. Neha and Ganeshan [13][14] presented the Elliptic Curve Cryptography (ECC) methodology for enabling encryption. By using a Diffie-Hellman key exchange mechanism the connection between the provider and user is established. It enables data integrity and minimize data loss and increases security.

Danwei et al. [15] presented a proposed encryption mechanism by splitting the data. In which the data are split by means of data splitting algorithm. Comparing to the existing traditional algorithms it restricts vulnerable to attacks and guarantees data reliability. The split data are stored and get back up in a separate single server which prevents from data loss. This mechanism effectively prevents brute force attacks.

Nayak et al., [16] presented a novel architecture in intending the cloud provider's trustiness by applying data reading protocol. Once confirming the provider is a trusted one, then only the data are stored. This proposed architecture comes with data backup's structure which set the backup data in different locations on the primary server. The author uses three algorithms such as data compressing is done by

means of GZIP algorithm, encryption by SHA Hash algorithm and files are split by using SFSPL algorithm.

Fig 4: The Architecture of Data Storing Security and Privacy

identifying the party. The major risk is integrity, confidentiality, and guarantees privacy preservation. Below tables will describe the

Mobile Cloud Data Storage Security and Privacy:

Mobile cloud computing is one of the fast growing technology. It is a combination of cloud computing, mobile computing, and wireless networks. The main motto of this Mobile cloud computing (MCC) is enabling rich mobile applications from internet applications. In these mobile devices are served as the cloud performing several intensive operations. The major problem in MCC is data ownership, privacy, and security. Let's discuss some of the related works on MCC;

Neeraj et al [27] presented Bayesian Coalition Game (BCG) mechanism for performing secure QoS management in the mobile cloud. In which RFID is used for enabling additional security in mobile computing. Sun [28] presented the major issues faced by cloud-based services in mobile devices. They are cloud pricing, scalability, security, code/computation offloading and task-oriented cloud services. To overcome these issues the author implemented a trust management system in mobile cloud computing. Yu and Wen [29] presented a new model for mobile computing. It minimizes the CPU usages on mobile resources, by enabling the more resources to be available in the mobile devices. Zegers et al., [30] presented a combination of lightweight encryption algorithm with the security handshaking protocol for the mobile devices. By this mechanism, the data security is ensured on the user side before the information's send to the cloud. This approach is not based on the third party authorization and succeeds with minimum communication overhead.

Conclusion:

In cloud computing there are several advantages like pay per use, a huge volume of space for storage, remote access from anywhere anytime, security and minimal cost facility on resource utilization, etc. As technology grows, several threats are increasing simultaneously. Most of the large organizations using cloud services for storing and accessing sensitive information's. In this industry there are multiple threats are still existing especially ensuring the data security in cloud environments. On the research platform, it considered as the major issues. In this paper, we have discussed several security and privacy issues in cloud computing as well as mobile cloud computing. Several tables demonstrate the technology comparison on the aspect of the methodology used, along with their characteristics, merits, and demerits. By means of these techniques, a proposed methodology is to develop in order to ensure data security as well as privacy in a detailed manner.

Summary of Cloud security and privacy challenges:

On the cloud environment, privacy is the major concern because of the cloud's distributed nature. Generally, the remote servers are conserved by the most trusted service providers. The account details in the service provider can conflict the security threats by means of comparison of various techniques involved in privacy, integrity, and confidentiality.

2. REFERENCES

1) Carroll, M., Van Der Merwe, A., and Kotzé, P. 2011. Secure cloud computing: Benefits, risks, and controls. 2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference.

2) P. Mell and T.Grance, "The NIST Definition of Cloud Computing", Natinal Institute of Standards and Techology, vol. 53, no.6, pp. 1-3, 2009.

3) M. Seibold and A. Kemper, "Database as a service," Datenbank- Spektrum, vol. 12, no. 1, pp. 59–62, 2012.

4) Leonard Heilig and Stefan Vob, "A Scientometric Analysis of Cloud Computing Literature", IEEE Transactions on Cloud Comouting, vol. 2, no. 3, pp. 266-278, July-September 2014.

5) Wenjie Liu , Peipei Gao, Zhihao Liu, Hanwu Chen, andMaojun Zhang "A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment" , Hindawi Security and Communication Networks Volume 2019, Article ID 4923590, 14 pages.

6) Y.Xu, L.Qi,W. Dou, and J.Yu, "Privacy-preserving and scalable service recommendation based on simhash in a distributed cloud environment," Complexity, vol. 2017, Article ID 3437854, 2017.

7) L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed localitysensitive hashing-based approach for cloud service recommendation from multi-source data," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2616–2624, 2017.

8) X. A.Wang, F. Xhafa,W. Cai, J.Ma, andF.Wei, "Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage," Computers and Electrical Engineering, vol. 56, pp. 871–883, 2016.

9) B.Wang,W. Song,W.Lou, andY.T. Hou, "Invertedindex based multi-keyword public-key searchable encryption with strong privacy guarantee," in Proceedings of the 34th IEEE Annual Conference on Computer Communications and Networks, IEEE INFOCOM 2015, pp. 2092–2100, Hong Kong, May 2015.

10) Srinivasa Rao Chintada, ChandraSekhar Chinta, "Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments", International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 3, pp. 3609-3616, March 2014.

11) Kaitai Liang and Willy Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage", IEEE Transaction on Informations Forensics and Security, vol. 10, no. 9, pp.1981-1992, September 2015.

12) R. Bala Chandar, M.S Kavitha, K seenivasan, "A Proficient Model for High end Security in Cloud Computing", ICTACT Journal on Soft Computing, vol. 4, pp. 694-702. January 2014.

13) Neha Tirthani, Ganesan R, "Data Security in Cloud Architecutre based on Diffie Hellmam and Elliptic Curve Cryptography, IACR Cryptology e-Print Archive, 2013.

14) Chen Yang, Furong Wang and Xinmei Wang, "Efficient Mediated Certificates Public-Key Encryption Scheme without Pairings", In the Proceedings of International Conference on Advanced Information Networking and Applications Workshops, AINAW, vol. 1, pp. 109-112, 2007.

15) Danwei Chen and Yanjun He, "A Study on Secure Data Storage Strategy in Cloud Computing", Journal of Convergence Information Technology, vol. 5, no. 7, pp. 175-179, September 2010.

16) K Badya Nayak, D Krishna, P Ravindra, "Data Integrity and Dynamic Storage Way in Cloud Computing", International Journal of Innovative Technologies vol. 3, issue. 2, pp. 0268-0273, ISSN: 2321-8665, June 2015.

17) Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable and Finegrained Data Access Control in Cloud Computing", In the Proceedings of INFOCOM, pp. 1-9, ISSN: 0743-166X, 2010.

18) M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable Secure File Sharing on Untrusted Storage", In the Proceedings of FAST, vol. 3, pp. 29-42, 2003.

19) Neeraj Kumar, Rahat Iqbal, Sudip Misra, Joel J. P. C. Rodrigues, M.S. Obaidat, "Bayesian Cooperative Coalition Game as-a-Service for RFID-Based Secure QoS Management in Mobile Cloud", IEEE Transactions on Emerging Topics in Computing, ISSN: 2168-6750, March 2016.

20) Zhongyuan Zhao, Mugen Peng, Zhiguo Ding, Wenbo Wang, and H. Vincent Poor, "Cluster Content Caching: An Energy-Efficient Approach to Improve Quality of Service in Cloud Radio Access Networks", IEEE Journal on Selected Areas in Communications, 2016.

21) Qian Wang, Cong Wang, Jin Li, Kui Ren and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", Computer Security–ESORICS, pp. 355-370, 2009.

22) Ping Hu, Chi Wan Sung, Siu-Wai Ho, and Terence H. Chan, "Optimal Coding and Allocation for Perfect Secrecy in Multiple Clouds",

IEEE Transaction on Information Forensics and Secuirty, vol. 11, no. 2, pp. 388-399, February 2016.

23) 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, pp. 468-477, Febraury 2014.

24) Huaqun Wang, Debiao He, and Shaohua Tang, "Identity Based Proxy- Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud", IEEE Transaction on Information Forensics and Security, vol. 11, no. 6, pp. 1165-1176, June 2016.

25) Yang, Zhi and Zhao, Ben Y and Xing, Yuanjian and Ding, Song and Xiao, Feng and Dai, Yafei, "AmazingStore: Available, Low-cost Online Storage Service Using Cloudlets", vol. 10, no. 6 pp. 1-5, 2010.

26) Xu, Xiaolong and Tu, Qun, "Data Deduplication Mechanism for Cloud Storage Systems", In the Proceedings of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 286-294, 2015.

27) Neeraj Kumar, Rahat Iqbal, Sudip Misra, Joel J. P. C. Rodrigues, M.S. Obaidat, "Bayesian Cooperative Coalition Game as-a-Service for RFID-Based Secure QoS Management in Mobile Cloud", IEEE Transactions on Emerging Topics in Computing, ISSN: 2168-6750, March 2016.

28) D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analysing Security, Privacy and Trust Issues in Cloud Computing Environments", Procedia Engineering, vol. 15, pp. 2852-2856, 2011.

29) X. Yu and Q. Wen, "Design of Security Solution to Mobile Cloud Storage", in Knowledge Discovery and Data Mining. Springer pp. 255-263, 2012.

30) William Zegers, Sang-yoon Chang, Younghee park and Jerry Gao, "A Light-Weight Encryption and Secure Protocol for Smartphone Cloud", IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 259-266, 2015.