International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-3, May 2021
https://doi.org/10.21276/ijircst.2021.9.3.12
Article ID IRP1164, Pages 70-73
www.ijircst.org

Cloud Storage Architecture: Issues, Challenges and Opportunities

Shalini Bhaskar Bajaj[1], Aman Jatain, Sarika Chaudhary[2], and Pooja Nagpal[3]

[1,2,3] Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Shalini Bhaskar Bajaj; shalinivimal@gmail.com

ABSTRACT - With the advent of new emerging technologies like fog computing, internet of things, blockchain, artificial intelligence etc, information and communication technology is revolutionising our homes, education, health and industry. By the year 2025, with the increase in network speed offered by 5G technology, we will be able to share much more data in real time. It's not only important to note that the volume of data shared in future will be huge but also its important to understand that the shared data will be heterogenous in nature. Not only humans but smart devices will act as humans on the network and will generate big data. Thus, the future of cloud storage industry seems to be very bright. The effort in this paper is to recognise the issues and challenges that the cloud storage industry will face in the near future and also to identify and review the new paradigm for researchers in the field of cloud storage.

KEYWORDS- Internet of Things, Artificial Intelligence, Security, FOG computing, Cloud Storage

I. INTRODUCTION

Advances in smart technology is resulting in a large amount of data generation and thus increasing in devices that are generating the data and thus increasing the investment in cloud by more than 331 billion dollars by 2023[1]. To implement this, improvement not only in storage infrastructure but also in processing techniques is required [2]. Advent of artificial intelligence and its integration in smart devices is further adding to the complexity in storing and processing data [1]. With the passage of time, more devices are added everyday to the internet to monitor and connect different buildings, traffic facilities lakes environment etc thus further increasing the size of data being generated on daily basis [3-7]. With the increasing data, it's becoming more challenging to store and process it [8, 9]. To handle unstructured data being produced at such a large scale, researchers are trying to device new databases based on new algorithms and softwares using NoSQL [10-12]. A number of frameworks have been proposed in the literature for storing and retrieving heterogenous /unstructured data in cloud storage environment [13-16]. With technological advancements, the computing and storage requirements of organisations are growing with time [17, 18]. This has given rise to "on demand storage" concept as the investment for setting up storage facility is very huge. But this leads to limited control over the computing resources as operations are performed through cloud over the internet [19, 20]. Storage services provisioning require cheaper, scalable and personalised solutions. Cloud storage issues include confidentiality, integrity, security, backup problem, vulnerabilities in virtualisation, data segregation, data access, data dynamics, authentication, data breaches, authorisations and many more. Section 2 of the paper focusses on issues related to cloud storage; section 3 discusses the future opportunities in cloud storage and the last section concludes the paper with key findings and the future directions.

II. DISCUSSION : CHALLENGES AND POSSIBLE SOLUTIONS IN CLOUD STORAGE

Infrastructure as a Service (IaaS): It is very crucial as mismanagement of proper storage facility in cloud may lead to severe consequences [21]. The cloud storage issues mentioned above are broadly divided into 2 categories: (a) issues related to data security, (b) issues related to data management.

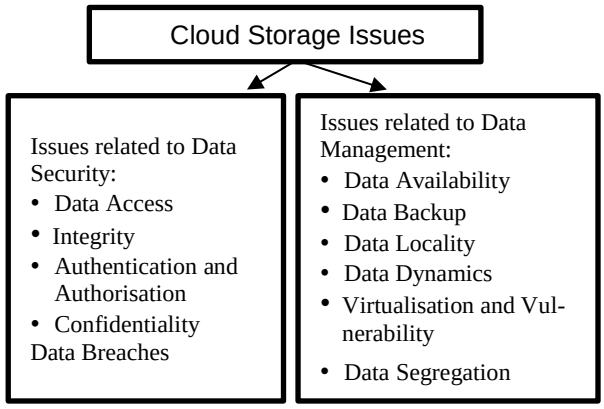

Fig. 1 Summary of Cloud Storage Issues

A. Issues related to Data Security

Any client using IaaS wants data security, as the data will be stored in the cloud storage. Therefore, companies providing IaaS are trying to design and develop new algorithms and frameworks that could provide controlled access to the cloud data. Moreover, the client has the right to know (i) whether the data deleted by them will be permanently deleted or still it can be accessed by the storage provider, (ii) where is actually the data stored in the cloud, and

many more such questions, as the client has limited or no control over the cloud storage.

B. Discussion on Data Access Issues

Issues related to accessing data in cloud environment are majorly related to security policies. A number of measures have been proposed in literature for dealing with the data access issues. These proposed measures can be classified into 3 broad categories: user-based, role-based and attribute-based access control [22, 23].

C. Discussion on Integrity Issues

Data integrity can be achieved by using constraints and transaction in a single database system. This can be easily achieved by transactions by using ACID properties of the database. In case of distributed database systems, multiple transactions are being executed on multiple databases. This leads to increased complexity of the system. In case of cloud computing scenarios, data integrity exponentially grows, as different types of application both local and Software as a Service (SaaS) are displayed as a service.

D. Discussion on Authentication and Authorisation Issues

Authentication plays an important role in allowing only those users to the cloud environment that are trusted ones. Depending on the sensitivity of the information stored on the cloud, authentication may be needed to access the information. The process of authentication needs to be efficient and robust and can be implemented using cryptographic techniques, thus, ensuring access to authenticated uses only [24-26].

E. Discussion on Confidentiality Issues

Confidentiality is achieved by using RSA algorithm based encryption and decryption techniques. Thus, the user must have access to the encryption and decryption keys. Whenever a sender wants to send a message to the receiver , sender signs the message with the sender key and then encrypts it with the public key of the receiver and downloads encoded text message. Once the receiver receives the message, it decrypts it with its public key. The confidentiality of the information stored in the cloud depends upon the privacy policies, terms of service provided by the cloud provider.

F. Discussion on Data Breaches

Cloud environment stores data of many users and thus any compromise in authentication and authorisation may lead to data breaches [11]. Since data of many organisations is stored in the cloud environment, it becomes quiet lucrative for attackers as entry to cloud environment means access to data of many organisations [27].

G. Issues related to Data Management

There ae number of data management issues related to cloud environment that has been categorised and explained below. These issues are: data availability, data backup, data locality, data dynamics, virtualisation and vulnerability, data segregation.

H. Discussion on Data Availability Issues

SaaS applications are available to the clients 24X7. Cloud storage must be able to handle DDOS (distributed denial of service attacks) and DOS (Denial of service attacks) [31-33].

I. Discussion on Backup Issues

In case of disaster situations, sensitive data must be backed up periodically by the SaaS providers for fast recovery in case any thing goes wrong. Strong encryption techniques must be used while taking backup so that accidental data leakages can be controlled. Tests to validate the backup provided by SaaS provider can be done by performing certain tests as: configuration insecurity, storage insecurity.

J. Discussion on Data Locality Issues

Clients in SaaS model, uses the application provided by the SaaS provider and its own data, but does not have the knowledge about the location of its data which may lead to data locality issues. As data stored in different countries is governed by the country's rule. Some countries do not allow migration of sensitive data out of their country.

K. Discussion on Data Dynamics Issues

Storing information and its management in cloud by performing tasks such as insertion, deletion and updation is not considered trustworthy as data and applications are stored in data centres. The protection of data is important in cloud environment as the data can be deleted by the cloud provider without the knowledge of the owner of the data. Errors in the software and data may be canceled by the cloud provider. This can be controlled by introducing auditing systems in cloud computing [28].

L. **Discussion on Virtualisation and Vulnerability Issues**

Segregating the different instances of same application running on a single machine is called virtualisation and is a major concern as far as security of client's information is concerned. Another important issue is of isolation and scalability. In case of virtual machines, root security is primary to avoid interference of host operating system with virtualised guest systems.

M. Discussion on Data Segregation Issues

The popularity of cloud computing is due to its multi tenancy nature [29, 30] wherein 'Software as a Service' (SaaS) facility offered by cloud environment allow multiple clients to store their data. This might lead to intrusion of one client's data by some other client as they share same softwares. SaaS has the responsibility to differentiate data of different users intelligently at both application and physical levels. Certain tests such as SQL injection flaws, storage security, data validations must be performed by the service provider to ensure proper segregation of data from different clients.

III. FUTURE OF CLOUD STORAGE AND OPPORTUNITIES

Due to the advent of AI, IoT devices, 5G connectivity and the amount of data being produced by such devices is changing the future of cloud and the way of living. This sub-section is going to discuss the future opportunities for the cloud storage:

A. Cost Effectiveness

With the advent of cloud computing environment, the cost of computing has gone drastically low as we can rent the storage space and resources of a supercomputer at very low cost.

B. Internet of Things

With the advent of IoT the number of devices has increased and their numbers are going to increase future at a very fast pace.

C. Accessibility in Remote Locations

Different cloud providers are providing remote access of data to their clients in a fast and reliable way. 5G services will further make the access to the data in a seamless manner.

D. Maximum Usability

Using drag and drop facility, the data can be stored and pulled between the local PC and cloud any number of times.

E. Future Connectivity

5G connectivity will ensure faster connectivity of client to different devices. Thus, we will be able to operate machines virtually sitting thousands of kms away.

F. Inclusion of Artificial Intelligence

Artificial Intelligence is making decisions in a number of situations from self driving cars to making complex decisions. Artificial Intelligence is making cloud storage more attractive and smarter and blockchain technology is further making it more secure.

G. Huge Data produced by Large Number of Devices

Approx. 75 billion devices will connect by the year 2025 and will be producing data at a very fast speed which will be stored and processed by cloud computing environments.

H. Collaboration and Sharing of Data

Whether it is a photo or a data file or any other file format, saying of files will become very easy with just few clicks. Work can be easily done in collaboration with other people sitting miles away without any issues.

I. Privacy and Security

Privacy and security is an important aspect of the cloud storage and is being maintained by firewalls, intrusion detection systems deployed in cloud, advanced encryption techniques, logging of various events.

J. Managing Disaster and Recovery

Data is the most powerful and at the same time most vulnerable resource at this point in time. If stolen, my lead to irrecoverable loss in income, productivity, customers, reputation and thus leads to loss in business.

K. Synchronisation and Automation

Automated data backup services are provided by the cloud providers.

IV. CONCLUSIONS AND FUTURE SCOPE

IT industry is being revolutionised very rapidly with the fast growing 5G technology, artificial intelligence, Fog computing, internet of things and other such upcoming technologies and their use with cloud environment. This paper mainly focussed on discussions based on challenges and possible solutions in cloud storage with issues related to data security and data management. It has been discussed that encryption techniques and block chain technologies can be deployed to enhance the security of the cloud storage and thus will make it more robust. Authentication techniques for access control may add an additional check point for capturing intruders to access the data stored on the cloud. In the end discussion on future of the cloud storage and various opportunities is done. The, we can conclude that cloud computing environment is a fast growing technology and is replacing the traditional computing environment. Efforts are being made in the direction of preserving the client's sensitive data by providing advance techniques and secure access features.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest

REFERENCES

[1] "Forbes: Cloud computing forecast," https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts2017/#5c42322c31e8/, 2020.

[2] X.Wang,B.Wang,andJ.Huang,"Cloud computing and its key techniques computer science and automation engineering(csae),"inInternationalConference on Cloud Computing. Shanghai, China: IEEE, 2011, pp. 404–410.

[3] W.Songyun,Y.Jiabin,L.Xin,Q.Zhuzhong,A.Fabio,andY.Ilsun ,"Active data replica recovery for quality-assurance big data analysis in ic-iot," IEEE Access, vol. 7, pp. 106 997 – 107 005, 2019.

[4] S.Karen,"Iot big data security and privacy versus innovation," IEEE Internet of Things Journal, vol.6, no.2, pp.1628–1635, 2019.

[5] S. Syed Attique, Z. S. Dursun, H. Sufian, and D. Dirk, "The rising role of big data analytics and iot in disaster management: Recent advances, taxonomy and prospects," IEEE Access, vol. 7, pp. 54 595 – 54 614, 2019.

[6] Q.Basheer,A.-F.Ala,A.Gupta,B.Driss,A.Safaa,and Q.Junaid,"Leveraging machine learning and big data for smart buildings: A comprehensive survey," IEEE Access, vol. 7, pp. 90 316 – 90 356, 2019.

[7] S. Rui, L. Shanyun, W. Shuo, X. Ke, and F. Pingyi, "Importance of small probability events in big data: Information measures, applications, and challenges," IEEE Access, vol. 7, pp. 100 363 – 100 382, 2019.

[8] B.Afzal, G.Anwar, S.Shahaboddin, A.Giuseppe, and P.Antonio, "Performance based service level agreement (psla) in cloud computing to optimise penalties and revenue," IET Communications, 2020.

[9] B. Afzal, S. Shahaboddin, G. Anwar, and C. Anthony, "Optimizing iaas provider revenue through customer satisfaction and efficient resource provisioning in cloud computing," IET Communications, vol. 13, no. 9, pp. 2913–2922, 2019.

[10] Ankita, V. Gregory, H. Seghbroecka, F. Morab, T. De, and V. Bruno, "Spech: A scalable framework for data placement of data-intensive services in geo-distributed clouds," Journal of Network and Computer Applications, vol. 142, pp. 1–14, 2019.

[11] Z.Lei,F.Anmin,Y. Shui, S. Mang and K.Boyu, "Data integrity verification of the outsourced big data in the cloud environment: A survey," Journal of Network and Computer Applications, vol. 112, pp. 1–15, 2019.

[12] A.Sidra,U.Saif,K.Abid,A.Mansoor,A.Adnan and K.K.Muhammad, "Information collection centric tech-

niques for cloud resource management:Taxonomy, analysis and challenges," Journal of Network and Computer Applications, vol. 100, pp. 80–94, 2019.
[13] W.-T. Tsai, Z. Jin, and X. Bai, "Internetware computing: issues and perspective," in Proceedings of the First Asia-Pacific Symposium on Internetware. ACM, 2009.
[14] H. Raj, R. Nathuji, A. Singh, and P. England, "Resource management for isolation enhanced cloud services," in Proceedings of the ACM workshop on Cloud computing security. ACM, 2009, pp. 77–84.
[15] V.Chang and G. Wills, "A model to compare cloud and non-cloud storage of big data," Future Generation Computer Systems, vol.57, pp.56–76, 2016.
[16] R. Kumar and A. K. Bose,"Internet of things and opc ua," ICNS 2015, p.52, 2015.
[17] S. Kamara and K. Lauter, Cryptographic Cloud Storage. Canary Islands, Spain: Springer Berlin Heidelberg, January 25-28 2010, pp. 136–149. [Online]. Available: http://dx.doi.org/ 10.1007/978-3-642-14992-4$_$13
[18] J. Ateeqa, B. Afzal, and R. Tauseef, "Sla based infrastructure resources allocation in cloud computing to increase iaas provider revenue," Research Journal of Science and IT Management, vol. 4, no. 3, pp. 37–44, 2015.
[19] P. Rajanetal.,"Evolution of clouds to rage as cloud computing infrastructure service," arXivpreprintarXiv: 1308.1303, no.1, 2013.
[20] R.Ghani-Ur, G.Anwar, Z.Muhammad, A. N. Syed Husnain and S. Dhananjay, "Ips: Incentive and punishment scheme for omitting selfishness in the internet of vehicles (iov)," IEEE Access, vol. 7, pp. 109 026 – 109 037, 2019.
[21] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Computer Communications, vol. 111, pp. 120–141, 2017.
[22] Sahai and B. Waters, "Fuzzy Identity-Based Encryption". Aarhus, Denmark: Springer Berlin Heidelberg, May 2005, pp. 457–473.
[23] E.-J.Goh, H.Shacham, N.Modadugu and D.Boneh, "Sirius: Securing remote untrusted storage." in NDSS, vol.3, 2003, pp.131–145.
[24] Z. Kartit, A. Azougaghe, H. K. Idrissi, M. El Marraki, M. Hedabou, M. Belkasmi, and A. Kartit, "Applying encryption algorithm for data security in cloud storage," in Advances in Ubiquitous Networking. Springer, 2016, pp. 141–154.
[25] D.Pritamand, M.Chatterjee, "Enforcingrole-based access control for secure data storage in cloud using authentication and encryption techniques," Journal of Network Communications and Emerging Technologies (JNCET), vol. 6, no. 4, 2016.
[26] L.Zhou, V.Varadharajan and M.Hitchens, "Enforcing role-based access control for secure data storage in the cloud," The Computer Journal, p. bxr 080, 2011.
[27] V.Chang and M.Ramachandran, "Towards achieving data security with the cloud computing adoption framework," IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138–151, Jan 2016.
[28] C.Wang, K.Ren, W.Lou and J.Li, "Toward publicly auditable secure cloud data storage services." IEEE network, vol.24, no.4, pp.19–24, 2010.
[29] A.Gholami and E.Laure, "Security and privacy of sensitive data in cloud computing: A survey of recent developments," arXivpreprintarXiv:1601.01498,2016.
[30] N.Ahmed,V.K.Ojha,andA.Abraham,"An ensemble of neuro-fuzzy model for assessing risk in cloud computing environment," in Advances in Nature and Biologically Inspired Computing. Springer, 2016, pp. 27–36
[31] R. K. Banyal, V. K. Jain, and P. Jain, "Data management system to improve security and availability in cloud storage," in nternational Conference on Computational Intelligence and Networks (CINE), Jan 2015, pp. 124–129.
[32] C.W.Chang,P.Liu,andJ.J.Wu,"Probability-based cloud storage providers selection algorithms with maximum availability," in 41st International Conference on Parallel Processing, Sept 2012, pp. 199–208.
[33] B.Mao, S.Wu and H.Jiang, "Exploiting work load characteristics and service diversity to improve the availability of cloud storage systems,"IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 7, pp. 2010–2021, July 2016.

ABOUT THE AUTHORS

Dr. Shalini Bhaskar Bajaj did her Bachelor of Engineering in Computer Science and Engineering from Deenbandhu Chhotu Ram University, Haryana, Master of Engineering in Computer Technology and Applications from Delhi Technological University and Ph.D. from Indian Institute of Technology Delhi (IITD), New Delhi. She worked with Liberty Footwear, India and Appware Technologies, LLC, Dubai as System Analyst. She worked as Professor with NCU and GD Goenka University, Gurgaon. She has to her credit twenty-two years of work experience on different projects, teaching and research in the field of Data mining. She has published more than fifty research papers in different national and international journals and presented paper in conferences. Her research interests include Data mining and Databases. Presently, she is working with Amity University Haryana as Professor and Head of Department, Computer Science and Engineering.

Dr. Aman Jatain has received her Ph.D from NCU University, M.Tech from Thapar University, Patiala and B.Tech from M.D U Rohtak. Since 2015 she is serving Amity University, Haryana as an Assistant Professor. Prior to this, she served ITM University as an Assistant Professor and also worked with Aricent Technologies as Software Engineer. She has more than 12 years of teaching and industry experience. Her research area includes Software Engineering, Data Mining, Networking, Machine Learning and Optimization Techniques. She has authored numerous technical research papers and book chapters in international conferences and journals of repute.

Ms. Sarika Chaudhary is currently working as Assistant Professor with Amity University, Haryana. She has published more than 34 research papers and 2 books. She is member of 16 Professional/Technical Committees and Editorial Board Member/Reviewer of 20 reputed Journals.

Ms. Pooja Nagpal, M. Tech (Computer Science & Engineering), B. Tech (Computer Science & Engineering) is working as Assistant Professor with Amity University Haryana