IX International Conference on Multidisciplinary Research
(IEI, Chandigarh) Institution of Engineers, India , Chandigarh
21st December 2019 www.conferenceworld.in
Conference World
ISBN : 978-81-943584-6-6

A Study on Map Reduce Based Secure and Fault Tolerance Data Migration in Cloud Computing

Sonal[1],Vijay[2]

[1]Neelkanth Institute of Engineering & Technology/ Abdul Kalam Technical University

ABSTRACT

Cloud Computing propose a new way of providing assets to users "as a service available via the internet". Transporting computing power(CPU, RAM, Network Speeds, Storage OS software) a service over a network is possible due to Cloud Computing. Data in the Cloud can be in various states: at-rest, in-use, in-transit.The data do not have the same level of security requirements. Data being processed can not be protected with the same means as data intransit or at rest. In a network, there is no complete security solution to secure data and app, or services, but satisfactory risk management can reduce the level of risks [27]. MapReduce is a programming system for distributed processing large-scale data in an efficient and fault tolerant manner on a private, public, or hybrid cloud. In this paper, we investigate and discuss security and privacy challenges and requirements, considering a variety of adversarial capabilities, and characteristics in the scope of MapReduce.

Keywords: Cloud, MapReduse, DataMigration.

INTRODUCTION:

Cloud Computing can be described as transporting computing power(CPU, RAM, Network Speeds, Storage OS software) a service over a network (usually on the internet) rather than physically having the computing assets at the customer location.A new way of providing assets to users "as a service available via the internet". Unlike traditional method that is occupied on hardware possesion where data is stored, Cloud Computing users no longer own the substructure that is totally precised by these service providers. The relocate of infrastructure restrict to the service providers involves the transmit of responsibility associatedwithdatasecurity[5,6,7,8,9,10].Therefore,datasecurityandprivacy concerns raise[1].

Cloud Computing is used in a variety of service models: SaaS, PaaS, IaaS: and deployment models: private, public, hybrid, community. Therefore, the risks are different depending on the level of cloud used; indeed, if the security control on a private Cloud is logically high since mastered, the level of control over a public Cloud is substantially lower. Likewise, whether the user depends on a software, platform or infrastructure,thelevelofcontrolisdifferentandthusthese security managementwillbe different. IaaS provides an infrastructure to host PaaS, which in turn provides a plat- form for developing and deploying SaaS applications; therefore, there is a security dependency between these layers.Moreover, Data in the Cloud can be in various states: at-rest, in-use, in-transit.The datadonothavethesamelevelofsecurityrequirements.Databeingprocessedcannot beprotectedwiththesamemeansasdata in transit oratrest.Encryption is the primary method used to protect the transmitted and stored data. This method is still valid today for Cloud environment. Yet, this solution is notalways possible as regard data-at-rest; In fact it is possible to encrypt a simple data in an IaaS service.However,it is not possible to encrypt data in a Paas or Saas application. Data-at-rest used by Cloud applications is usually unencrypted because encryption prevents data indexing and searching. This is the case for data-in use that must be in a clear form for many applications [11,12,13,14].

The use of encryption alone is not sufficient to

secure this type of data concerning data in transit; Indeed, confidentiality is guaranteed by encryption but not integrity [13]. Therefore, encryption algorithms are generally coupled with security protocols as well as network security equipment [11, 7, 13, 15]. Moreover, data-at-rest and the data-in-transit encryption techniques may be different. For example, the encryption keys for the data in transit may be of short duration, while the keys for the data-at-rest may be preserved during a longer period [16].Otherwise, sizeand data type are the parameters on which data security solution depend. Indeed, the conventional solutions for securing a small set of data maybe not suitable for large volume of data, like encryption. Regardingdata type, confidentiality is required sensitive data while privacy is required by personal data. The information that must be protected in sensitive data is the contentof data that were generally achieved by encryption techniques. Availability and integrity are required more or less by all data types[1].

In the process of maintaining verifiable results to offload the computation of a function to other perhaps untrusted servers,A computing device is enabled by the provable computing.The function is checked out by the other servers and aevidence of correct computation of the function is returned. In [17], the term confirmable computing was structured.A user is now capable to securelook for over encrypted data through keywords without decryption because several schemes that can be searched have been developed by the researchers.

In[18], the first ever scheme for searchers on encrypted data had been planned by the authors, by which, the varifiable privacy for encryption, query isolation, controlled probing and maintain of unseebquery is provided. Researchers have developed many other schemes later on, such as [19,20]

The privacy of location of the fog clients is derived by the location privacy mainly.As The tasks of a fog client generally dropped to nearby fog node. And that fog node can infer that the client is nearest and other fog node is farthest then it.additionally, if multiples fog services is beused by a fog client at dissimilar locations, Assuming the fog node join together, its way track might be leak by fog node.As long as A person or an important object is closed with such a fog client, their location privacy is at danger.

If a nearby fog server is rigorously being selected by the fog client, the fog node can certainly know that the fog client that is utilize its computing resources is nearest.

Individualityconcealing is the only way to preserve the location privacy such that fog node can't recognize the fog client even if it knows fog client is nearest. Individuality concealing can be done by a variety of methods For example ,In [21], A confidential third party is second-hand by the author to produce forged id for every end user. In fact, there is no necessarly that a fog client select the near by fog node but the fog node is selected according to some criterion such as latency, status, load balance etc.In this case, the tough location of fog client can be known by the fog node but can't do it so exactly.However, the location of a fog client boil down to a small section when fog client utilize computing resources from multiple fog nodes in an region, since the location of the fog client must be in the interchange of the multiple fog node's coverage.In such scenario, method used in [22] can be second-hand to protect the location privacy.Some trust domain usually address the traditional access control.

In that same trust domain traditional access control usually addressed. While the nature of cloud computing is outsource, so for outsourced data the implementation of the retrieve control in cloud computing is mostly cryptographic. In key management the symmetric key based solution is not upgradable. Fine grained retrieve control is being attained by several public key based solutions.

On attribut based encryption (ABE), A fine grained data retrieve control scheme is structured as [23] has prospected. In fog computing, a policy based resource retrieve control is prospected by work, to support protectassociation and ability to exchange and use information between heterogeneous resources [24]. It will be hard to know how to design retrieve control connection client-fog-cloud at the same time to meet structural goals and resource restraints [25].

In cloud computer the largestissue is security [26]. To secure data and app or services there is no

finished security solution in a network, but the dangers level can be decreased by agreeable risk management [27].

protective the data from unauthorized users, stopping modifications and limiting the retrieve of delicate information is the process of information or data security [28].

Some computes are related with cloud computing such as the framework of cloud provider must be secure and at the same time customer must assure that provider has taken proper security computes to protect their information. The protection of cloud user from the provider is the last security evaluate.

In cloud computing To protect security a correct and regular understanding and analysis of safety evaluation is needed. "A set of policies, technologies and controls expend to protect data, applications and the related framework of cloud computing is defined as Cloud Computing security"[29].

To support the communication between the cloud application and the environments, as well as to go faster the deployment and support of those cloud applications that need scalability, the providers of the cloud software environments supply the developers with a programming language level environment with a set of well described APIs[30][31].

As platform as service (PaaS)[32] commonly refers the service provided by cloud system in this layer. Google's App Engine is one of the examples of system in this category. A runtime environment and APIs is provided by that system.The use of AES that is provided in [33] is the solution to secure storage of the records in data base, which should take optimal time for storage and is prone to less security attacks. It is very complex for attacks because the key will be rotation mode based on the implementation of simple logic in the algorithm.

Without knowing content of original file, the encrypted file for both the owner and the receiver can be converted by the proxy servers[34].Even all the access permissions made by the owner himself and any kind of attack can not harm these schemes. In [35],the opportunities for cryptography to address the security challenges in the area of communication, cloud storage and virtualization is given.To improve The performance of cryptography, A technique known as The parallel computing is analyzed in [36] and the strategies used in parallel computation are mainly divide and conquer strategy. The sequential computation can not provide better results then the parallel computation. In [37], data access prevention from unauthorized access is discussed and a scheme to perfectly store the data and identifies the temper at the cloud server is proposed.Data updating, appending and deleting tasks are also performed by it.In [38], the data storage correctness in reference of cloud computing is analyzed.For trusted and secure data storage model they have provided an algorithm with new encryption scheme and integrity verification.To give all the solutions for trusted and secure data storage on cloud and to reduce computational cost the features of algorithm are useful.A scheme, double layer encryption means "Two layer encryption" was proposed in [39] for securely outsourcing the data in the cloud.

The cloud will decrypt the outer layer and the user will be the one who will decrypt the inner layer.The information/data will be highly secured by this manner.The advantages and drawbacks of several storage techniques that provide security to data in cloud are studied in [40].NubiSave was introduced in [41], it is a user friendly storage controller implementation with adaptable overheads and it runs on and integrates into typical consumer environments as a central part of an overall storage.For achieving optimality in cloud storage services along the provider's and consumer's iteration of the service life cycle a systematic approach also presented in [41].According to Apache Hadoop project, the distributed processing of large data sets on compute clusters of commodity hardware can be done by software framework named as HadoopMapReduce [42].The applications running over the Internet such as (software as a service)SaaS or hardware systems in data centers are under focus of the emerging field of information technology. In both the cases, services rendered by data centers and data management are not fully trustworthy.We have had comparison between the sequential method and the parallel method.In the current cloud Era several security issues have been identified.

At the time of fetching data from different servers/security for distributed cloud computing the data is not safe.

A migration technique that should be secure and non faulty is necessarily required by which the data can be transferred securely between the servers using MapReduce based algorithm.We will try to implement and compare the proposed idea in our

future work to resolve the current problems identified in this paper that helps in making cloud computing data migration and retrieval fault tolerant and more secure with high efficiency.

CONCLUSION

Cloud Computing propose a new way of providing assets to users "as a service available via the internet". Transporting computing power(CPU, RAM, Network Speeds, Storage OS software) a service over a network is possible due to Cloud Computing. Data in the Cloud can be in various states: at-rest, in-use, in-transit.The data do not have the same level of security requirements. Data being processed can not be protected with the same means as data intransit or at rest. In a network, there is no complete security solution to secure data and app, or services, but satisfactory risk management can reduce the level of risks [27]. MapReduce is a programming system for distributed processing large-scale data in an efficient and fault tolerant manner on a private, public, or hybrid cloud. In this paper, we investigate and discuss security and privacy challenges and requirements, considering a variety of adversarial capabilities, and characteristics in the scope of MapReduce.

REFRENCES

[1] "An Overview on Data Security in Cloud Computing",LyndaKacha and AbdellhafidZitouni,Advances in Intelligent System and Computing 661, DOI 10.1007/978-3-319-67618-0_23.

[2] "Security and Privacy Issues of Fog Computing:A Survey",Shanhe Yi,Zhengrui Qin,and Qun Li,Springer International Publishing,DOI 10.1007/978-3-319-21837-3_67,Issn:0302-9743,August 2015.

[3] "Survey on Cloud Computing and Security Issues" Rajeswari[1], Vinitha R[2], Greeshma N[3] ,International Journal of Innovative Research in Computer and Communication Engineering, Vol.6,Issue 4,April 2018.

[4] "Evaluation and Comparison of Security Issues on Cloud ComputingEnvironment",PriyankaArora,ArunSingh,HimanshuTyagi,World of Computer Science and Information Technology journal(WCSIT)ISSN:2221-0741Vol.2,No.5,179-183,2012

[5] An, Y.Z., Zaaba, Z.F., Samsudin, N.F.: Reviews on security issues and challenges in cloud computing.In:IOPConferenceSeries:MaterialsScienceandEngineering,vol.160, p. 012106. IOP Publishing(2016)

[6] Bhabad, A.V., Heda, J.R., Dhatrak, V.N., Shahane, G.P., Shirole, B.S: Data confidentiality andsecurityinCloudComputingusingKISTalgorithm.Int.J.Emerg.TrendsSci.Technol. 1 (2016).2456-0006

[7] Albugmi,A.A.,Alassafi,M.O.,Walters,R.,Wills,G.:Datasecurityincloudcomputing.In: IEEE Fifth International Conference on Future Generation Communication Technologies, pp. 55–59. IEEE(2016)

[8] Munier, M., Lalanne, V., Ardoy, P.Y., Ricarde, M.: Métadonnées et aspects juridiques: vie privéevssécurité de l'information. In: 9ème Conférencesur la Sécurité des Architectures RéseauxetdesSystèmesd'Information,pp.65–76.SARSSI(2014)

[9] Tchifilionova,V.:Securityandprivacyimplicationsofcloudcomputing-lostinthecloud.In: Springer Open Research Problems in Network Security, pp. 149–158. Springer, Heidelberg (2011)

[10] Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. Int. J. Internet Serv. Appl.1, 7–18 (2010)

[11] CercleNumérique des Industries Stratégiques (2012). http://cnis.afnet.fr/commissions/juridique/commission-juridique-nb02-aspects-juridiques-du-Cloud-Computing/commission- juridique-aspects-juridiques-du-Cloud-Computing

[12] 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)

[13] 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)

[14] Shaikh, R., Sasikumar, M.: Data classification for achieving security in cloud computing. Proc. Comput. Sci. 45, 493–498(2015)

[15] Roy, N., Jain, R.: Cloud computing: architecture and concept of virtualization. J. Sci. Technol. Manag. 4 (2015).2394-1537

[16] Tchifilionova,V.:Securityandprivacyimplicationsofcloudcomputing-lostinthecloud.In: Springer Open Research Problems in Network Security, pp. 149–158. Springer, Heidelberg (2011)

[17] Gennaro,R.,Gentry,C.,Parno,B.:Non-interactiveverifiablecomputing:Out-sourcingcomputationtountrustedworkers.In:CRYPTO.Springer(2010)

[18] Song,D.X.,Wagner,D.,Perrig,A.:Practicaltechniquesforsearchesonencrypted data. In: Security and Privacy. IEEE (2000)

[19] Wang,C.,Cao,N.,Ren,K.,Lou,W.:Enablingsecureandefficientrankedkeyword search over outsourced cloud data. TPDS 23(2012)

[20] Cash,D.,etal.:Dynamicsearchableencryptioninvery-largedatabases:Data structuresand implementation.In:NDSS.vol.14(2014)

[21] Wei,W.,Xu,F.,Li,Q.: Mobishare: Flexible privacy-preserving location sharing in mobile online social networks. In:INFOCOM. IEEE(2012)

[22] Gao,Z.,Zhu,H.,Liu,Y.,Li,M.,Cao,Z.:Locationprivacyindatabase-drivencog-nitive radio networks: Attacks and countermeasures. In: INFOCOM. IEEE (2013).

[23] Yu,S.,Wang,C.,Ren,K.,Lou,W.:Achievingsecure,scalable,andfine-grainedataaccesscontrolincloudcomputing.In:INFOCOM.IEEE(2010)

[24] Dsouza,C.,Ahn,G.J.,Taguinod,M.:Policy-drivensecuritymanagementforfogcomputing:Preliminaryframeworkandacasestudy.In:IRI.IEEE(2014)

[25] Bonomi,F.,Milito,R.,Zhu,J.,Addepalli,S.:Fogcomputinganditsroleinthe internetofthings.In:workshoponMobilecloudcomputing.ACM(2012)

[26] MutumZicoMeetei- Cloud Computing and Security Measure. International Congress on Image and Signal processing (CISP),2013.

[27] Gaurav Jain, VikasSejwar – Improving the Security by using Various Crypto GraphicTechniques in CloudComputing. International Conference on Intelligent Computing and Control Systems (ICICCS),2017.

[28] S.Rajeshwari, R.Kalaiselvi-Survey of data and storage security in cloud computing. In proceedings of the IEEE International Conference on Circuits and systems (ICCS),PP.76-81,2017.

[29] Anil Barnwal, SatyakamPugla, Rajesh Jangade Various Security Threats and their Solution in Cloud Computing International Conference on Computing Communication and Automation (ICCCA),2017.

[30] Lamiayouseff,MariaButrico,Dilma Da Silva,"Toward a UnifiedOntology of Cloud Computing,in2008,http://www.cs.ucsb

[31] 3tera,http://www.3tera.com,April 2009,"Cloud computing for web Applications."

[32] JunjiePeng,XuejunZhang,ZhouLei,BofengZhang,QingLi,"Comparison of Several Cloud Computing Platforms,"inSecondInternational Symposium on Information Science and Engineering,2009 I

[33] Anitha, P. and Palanisamy, Data protection Algorithm Using AES, *International Journal of*

Current Research, 2011 *vol.3, issue 6*, pp.291-294.

[34] ChaitanyaP.Sahithi and M.Murali, Improved Schemes to Secure Distributed Data Storage against Untrusted Users, *International Journal of Computer Science and Information Technology(IJCSIT)*, 2014,*vol.5(2)*, pp.1774-1777.

[35] ChauhanNitin Singh and AshutoshSexena, *Cryptography and Cloud Security Challenges*, CSI Communications, 2013, pp. 18-20.

[36] Nagendra M. and M. Chandra Sekhar , Performance Improvement of Advanced Encryption Algorithm using Parallel Computation, *International Journal of Software Engineering and its Application(IJSEIA)*,2014, *vol. 8, no 2*, pp.287-296.

[37] PurushothamanDeepanchakaravarthi, SunithaAbburu, 2012.An Approach for data Storage Security in Cloud computing, *International Journal of computer science Issues(IJCSI), vol.9, issue 2*, no 1, pp.100-105.

[38] RajawatJitendra Singh, Sanjay Gaur,2013.Trusted and Secure Model for Cloud Storage, *Journal of Environment Science, Computer Science and Engineering & Technology(JECET), vol.2, no 3*, pp.883-888

[39] RahulkarBhavesh , Praveen Shende,2013.A Two layer encryption Approach to Secure Data Sharing in Cloud Computing, *International journal of Advanced Research in Computer Engineering and Technology(IJARCET), vol.2, issue 12*, pp. 3252-3254.

[40] Sivashakthi T. and Dr. N Prabakaran, A Survey on Storage techniques in Cloud Computing, proceedings of *IJETAE*,2013, vol. 3, issue 12, pp.125-128.

[41] Spillner Josef, Johan Muller and Alexander Schill, 2013.Creating optimal cloud storage systems, *Future Generation Computer Systems*, pp.1062-1072.

[42] Apache Software. (2013) Mapreduce tutorial. Accessed: 2018-08-23. [Online]. Available: https://hadoop.apache.org/docs/r1.2.1/mapredtutorial.html#MapReduce+-+User+Interfaces