JES Journal of Engineering Sciences

Vol 10, Issue 11, Nov /2019
ISSN NO:0377-9254

INTEGRATING WITH FOG COMPUTING FOR PRIVACY PRESERVING OF DATA SHARING IN THE CLOUD

RAVURI SRINATH [#1], KARINKI SURYA RAM PRASAD [#2] , D.D.D SURI BABU [#3]

[#1] M.Tech Student, [#2] Assistant Professor, [#3] Head & Associate Professor
Department of Computer Science and Engineering,
DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi,Bhimavaram - 534202.

ABSTRACT

As there was a tremendous growth of unstructured data, cloud storage technology gets more attention and better development. However, in current storage schema, user's data is totally stored in cloud servers. In other words, users lose their right of control on data and face privacy leakage risk .In this proposed thesis we finally try to design a Three Layer Approach in order to store and access the data in a secure manner from the cloud server. Here we have integrated Fog Server concept for the current cloud in which the data can be stored on a multiple nodes rather than all the data in a single storage medium. Here we try to divide the data into multiple blocks in which each and every block is encrypted by the data owner. Once if any data user try to access the file, he need to request the file access from the cloud server in which the cloud server will try to give access permission for multiple blocks and once if the cloud server provide access those users can view the file in a decrypted manner and remaining who are not having permission from multi level,the data cannot be viewed in a plain text manner.

I. INTRODUCTION

Cloud computing is the utilization of processing assets (equipment and programming) that are conveyed as an administration over a system (normally the Internet). The name originates from the regular utilization of a cloud-formed image as a deliberation [1] for the perplexing foundation it contains in framework outlines. Distributed computing endows remote administrations with a client's information, programming and calculation[2]. Distributed computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations regularly give access to cutting edge programming applications and top of the line systems of server PCs[3].

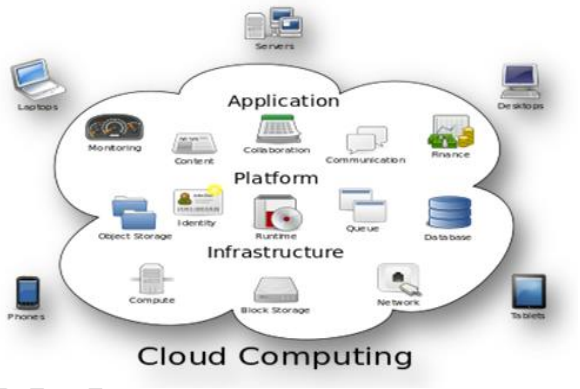


Figure.1 Represents the Structure of Cloud Computing.

Working

The objective of distributed computing is to apply customary supercomputing, or superior registering power, ordinarily utilized by military and research offices, to perform several trillions of calculations for every second, in buyer situated applications, for example, money related portfolios, to convey customized data, to give information stockpiling or to influence vast, vivid PC amusements[4]. The distributed computing utilizes systems of extensive gatherings of servers ordinarily running ease purchaser PC innovation with specific associations with spread information preparing errands crosswise over them. This mutual IT framework contains huge pools of frameworks that are connected together. Regularly, virtualization methods are utilized to augment the intensity of distributed computing[5].

II. LITERATURE SURVEY

P. Mell and T. Grance Cloud computing is a model for enabling 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models[1].

H. Li, W. Sun, F. Li, and B. Wang Cloud computing[4] has been gradually considered the most significant turning point in the development of information technology during past few years. People reap the benefits from cloud, such as ubiquitous and flexible access, considerable capital expenditure savings, pay-as-you-go computing resources configuration, etc. Many companies, organizations, and individual users have adopted the public cloud storage service to facilitate their business operations, research, or everyday needs. However, in the outsourcing cloud computing model, users' physical control of the underlying infrastructure including the system hardware and lower levels of software stack, is shifted to third-party public cloud service providers, such as Dropbox, Google Drive, Microsoft SkyDrive and so on. In addition, the sensitive data of users are also outsourced to and stored in the cloud, e.g., they may upload emails, photos, financial reports, and health records to the cloud[11]. Thus, the potential private information leakage and integrity of the outsourced data is one of the primary concerns for the cloud users. This paper focuses on the enabling and critical cloud computing security protection techniques and surveys on the recent researches in these areas. In addition, we further point out some unsolved but important challenging issues and hopefully provides insight into their possible solutions.

M. H. Au, W. Susilo, and Y. Mu Dynamic k-times mysterious confirmation (k-TAA) plans enable individuals from a gathering to be verified secretly by application suppliers for a limited number of times, where application suppliers can freely and powerfully concede or repudiate get to ideal to individuals in their very own gathering. In this paper, we build a dynamic k-TAA plot with existence complexities of O(log(k)) and a variation, in which the confirmation convention just requires consistent reality complexities at the expense of O(k) - measured open key. We additionally portray some tradeoff issues between various framework attributes. We detail all the zero-information confirmation of-learning conventions included and demonstrate that our development is secure in the arbitrary prophet display under the q-solid Diffie– Hellman presumption and q-decisional Diffie– Hellman reversal suspicion. We give a proof-of-idea execution, investigate its execution, and demonstrate that our plan is viable[6].

III. OBJECTIVE

The main objective to design this proposed thesis is to provide multi-level cloud storage in an open environment for storing and accessing the data in a secure manner. To provide encryption and decryption of data while uploading and downloading the data to and from the cloud servers. To provide multi level data storage in order to store the data in a de-centralized manner rather than in a centralized manner.

IV. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like dividing the data into multiple blocks and store the individual blocks on a separate storage medium like cloud server,fog nodes and local servers[7]. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the existing cloud servers all the data can be viewed and accessed by anyone who is having an account access within the cloud, so that the data is not having integrity or security in terms of any modification or changes done by any user. Also in the existing cloud servers there is no concept like three layer approach for privacy preserving of cloud data storage in order to process computational processing for an intelligent decision making.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They is as follows:

1. All the existing schemes are accessed information only in a plain text manner rather than in a encrypted manner.
2. All the current cloud servers has search in a normal manner under plain text model, but they don't have any facility to search in a secure manner
3. The existing cloud servers are almost operated in a centralized manner, where all the access can be viewed and monitored by the cloud service providers.
4. There is no concept like multi layer approach for privacy preserving of data under de-centralized manner.

V. PROPOSED SYSTEM

As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption andno facility like dividing the data into multiple blocks and store the individual blocks on a separate storage medium like cloud server [8], fog nodes and local servers. In this proposed thesis, we try to design a secure approach in which data can be divided into multiple partitions and store those multiple parts on an individual fog nodes in order to store and access in a secure manner.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. In this proposed schemes the information is accessed in an encrypted manner rather than in a plain manner.
2. All the current cloud servers has the facility to store and access the data in a secure manner.
3. The proposed cloud servers are almost operated in a de-centralized manner, where all the access of data cannot be possible by the cloud service providers.
4. There is no concept like multi layer approach for privacy preserving of data under de-centralized manner.

VI. HMAC ALGORITHM

HMAC is known as Hash Message Authentication Code Algorithm [9] which is used for generating the hash keys which are required for the identity of data blocks. This is used in this current application in order to identify the blocks uniquely by the individual storage areas[10].

The following are the step by step procedure for the HMAC algorithm

STEP 1: Append zeros to the left end of K(shared key) to create a b-bit string K+ (for example, if K is of length 160 bits and b = 512, then K will be appended with 44 zero bytes 0x00).

STEP 2: XOR (bitwise exclusive OR) K+ with ipad to produce the b-bit block Si.

STEP 3: Append M to Si.

STEP 4: Apply Hash function to the stream generated in Step 3.

STEP 5: XOR K+ with opad to produce the b-bit block So.

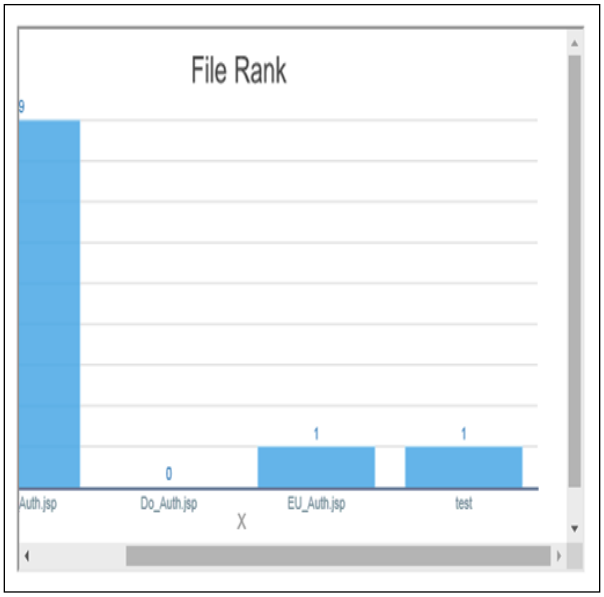
STEP 6: Append the hash result from Step 4 to So.

STEP 7: Apply Hash function to the stream generated in Step 6 and output the result.

VII. EXPERIMENTAL RESULTS

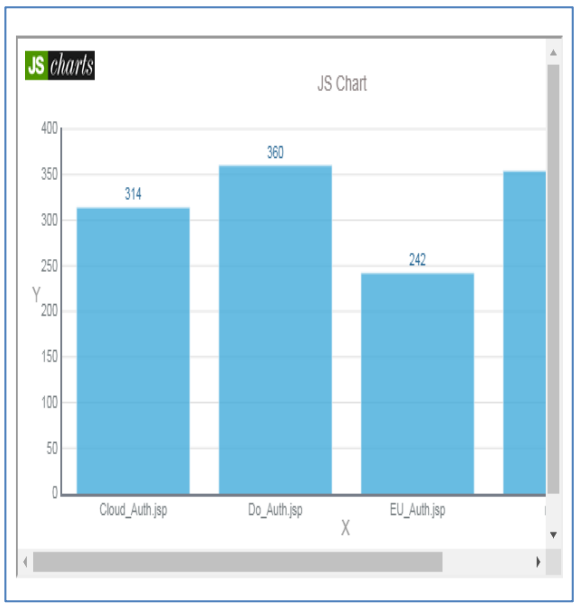
In this section we try to implement the proposed concept on multi-level cloud data storage and prove the data is stored in a secure manner.

User Can View the Rank of Each and Every Individual File



Here the user will get the files in a ranked manner based on the number of users

User Can View the Time Delay for Each and Every File



Here the user will see the delay time for each and individual file for uploading into the cloud server. This time delay is measured in terms of milliseconds.

Here the user will see the throughput time for each and individual file for getting response for the data owner. This time delay is measured in terms of milliseconds.

VIII. CONCLUSION

In this paper, we have integrated fog server concept for the current cloud in which the data can be stored on a multiple nodes rather than all the data in a single storage medium. Here we try to divide the data into multiple blocks in which each and every block is encrypted by the data owner. Once if any data user try to access the file, he need to request the file access from the cloud server in which the cloud server will try to give access permission for multiple blocks and once if the cloud server provide access those users can view the file in a decrypted manner and remaining who are not having permission from multi level, the data cannot be viewed in a plain text manner. By conducting various experiments on our proposed protocol, our comparison results clearly tell that our proposed approach is best in providing security for the sensitive data which is stored inside the server space.

FUTURE WORK

As a future work we try to further improve the efficiency while keeping all nice features of the system. In future we try integrate more and more additional stages for the cloud server in order to provide extra security for the data which is stored inside the cloud server.

IX. REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50, 2009.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloudcomputingenvironments,"inProc.IEEEInt.Conf. Commun.,2014, pp. 2969–2974.

[4] H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop., vol. 51, no. 7, pp. 1397–1409, 2014.

[5].Li,T.Wang,G.Wang,J.Liang,andH.Chen,"Efficient datacollection in sensor-cloud system with multiple

mobile sinks," in Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf., 2016, pp. 130–143.

[6] L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process., vol. 31, no. 3, pp. 464–472, 2016.

[7] R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," Commun. ACM, vol. 24, no. 9, pp. 583–584, 1981.

[8] J. S. Plank, "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol., 2005, pp. 1–74.

[9]Kulkarni,A.Forster,andG.Venayagamoorthy,"Computationalintelligenceinwirelesssensornetworks:Asurvey," IEEE Commun. Surv. Tuts., vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10]z.xia And K.ren "A privacy Preserving and copy deterrence content based image retreieval scheme in cloud computing in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Comput., vol. 41, pp. 219–230, 2017.

X. ABOUT THE AUTHORS

RAVURI SRINATH is currently pursuing his 2 Years M.Tech in the Department of Computer Science and Engineering at DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi, Bhimavaram - 534202.His area of interest include the Networking, Cloud Computing and Big Data.

KARINKI SURYA RAM PRASAD is currently working as an Assistant Professor in the Department of Computer Science and Engineering at DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi, Bhimavaram - 534202.He has more than 5 years of teaching experience in various engineering colleges. His research interest includes Networks, Data Mining, UML, UNIX and Pattern Design.

D.D.D SURI BABU is currently working as an Head and Associate Professor in the Computer Science and Engineering at DNR College of Engineering and Technology, Sri RamaPuram, Balusumudi, Bhimavaram - 534202.He has more than 15 years of teaching experience in various engineering colleges. His research areas include the Data Mining, Cloud Computing and Big Data..