IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A secure Blockchain-Based Scheme for Cloud Data Security Using Fog Computing

GUDIWAKA VIJAYALAKSHMI [#1], GARIKINA BHUVAN CHANDAR[#2]

[#1] Assistant Professor, Department of Computer Science and Engineering, Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh.

[#2] MCA Student, Department of Computer Science and Application, Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh.

vlgudiwaka@gmail.com [#1] , Bhuvanchandar143@gmail.com [#2]

ABSTRACT

Due to the high need for unstructured data storage nowadays, cloud storage technology is crucial for storing and accessing data on remote servers for better growth. Due to a lack of security, there are several privacy leakage issues in use today's cloud storage services. There is a potential that unauthorised users might misuse the data by deleting or altering the data that already exists in the data repository because, in general, all cloud servers attempt to store and access the data under a centralised storage location. This inspired me to suggest this essay, which incorporates fog computing to completely secure the data. Here, we created a multi-level privacy protection system where each and every portion of a cloud server that is divided into pieces is viewed as a fog node The data will be split up into several chunks at first, and each block is individually and securely deposited into a fog node. Here, the data that is saved on the cloud server was encrypted and decrypted using the block chain technology. We ultimately arrived to the conclusion that our suggested SBBS is effective at protecting cloud data from unauthorised user access by running several experiments on our proposed model, and if this is launched in cloud servers, there will be significant security for the distant data.

KEYWORDS:

Cloud Server, Fog Computing, Centralised Storage, Security.

1. INTRODUCTION

An new technology known as cloud computing was initially presented by San Jose in SES 2006 (Search Engine Strategies 2006) and defined by NIST (National Institute of Standards and Technology) [1]. Since it was first introduced, cloud computing has garnered a lot of interest from many facets of society. Through the efforts of so many people, cloud computing has developed throughout time [2]. A few cloud-based technologies are also derived from cloud computing. One significant component of these is cloud storage. The amount of user data is growing geometrically as network capacity expands quickly [3]. User

requirements can no longer be met by the capabilities of the local machine. People search for novel ways to save their data as a result. An increasing number of people use cloud storage in search of more powerful storage capacity. The future of data storage is on public cloud servers, and in a few years, cloud storage technologies will become widely used. A cloud computing system called "cloud storage" offers data management and storage services.

Cloud storage enables a large number of various storage devices to cooperate in a coordinated manner thanks to a cluster of applications, network technology, and distributed file system technology [4], [5]. Many businesses today provide a range of cloud storage services, including Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These businesses provide big storage capacities and a variety of features relating to other well-liked applications, which ultimately contributes to their success by drawing amusing subscribers. However, there are still several security issues with cloud storage services. The privacy issue is the most important of those security concerns.

The future of data storage is on public cloud servers, and in a few years, cloud storage technologies will become widely used. A cloud computing system called "cloud storage" offers data management and storage services. Cloud storage makes a lot of various storage devices cooperate in concert thanks to a cluster of apps, network technology, and distributed file system technology [4], [5]. Many businesses today provide a range of cloud storage services, including Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These businesses provide big storage capacities and a variety of features relating to other well-liked applications, which ultimately contributes to their success by drawing amusing subscribers. However, there are still several security issues with cloud storage services. The privacy issue is the most important of those security concerns.There have been a few well-known instances of cloud storage privacy leaks in the past.

For instance, during the Applesi Cloud Leakage Event in 2014, countless private images of Hollywood women were taken. The consumers' concerns about the privacy of their data kept on cloud servers were brought on by this controversy, which is what created the uneasiness. The user directly uploads data to the cloud server. As a result, users do not really have control over how their data is physically stored, which separates ownership and administration of data [6]. The data kept in the cloud is open to the CSP's unfettered access and searching.

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the new application or model, it's necessary to work out the time factor, economy and company strength. Once all these factors are confirmed and got an approval then we can start building the application.

MOTIVATION

1) "The NIST definition of cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, 2009, pp. 50–51.

Authors: P. Mell and T. Grance

A shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly deployed and released with little administration work or service provider involvement is made possible by the cloud computing concept. Three service models, four deployment methods, and five key criteria make up this cloud model.

2) "Secure and privacy-preserving data storage service in public cloud," Journal of Computing Research and Development, vol. 51, no. 7, pp. 1397–1409, 2014.

Authors: H. Li, W. Sun, F. Li, and B. Wang

Over the past several years, the growth of cloud computing has gradually come to be recognised as the most significant turning point in the history of information technology. People profit from the cloud in a variety of ways, including ubiquity and flexibility of access, significant capital cost reductions, pay-as-you-go computing resource configuration, etc. The public cloud storage service has been used by several businesses, organisations, and individual users to support daily operations, research, or other purposes. The users' physical management of the underlying infrastructure, including the system hardware and lower layers of the software stack, is instead transferred to external public CSPs under the outsourcing cloud computing model.

3) Dynamic constant-size k-TAA

Authors: M. H. Au, W. Susilo, and Y. Mu

Individuals from a group can be verified covertly by application providers for a certain number of times using dynamic k-times mysterious confirmation (k-TAA) schemes, where application providers can freely and forcefully grant or deny access rights to anyone in their own group. In this study, we construct a dynamic k-TAA plot with existence complexities of O(log(k)) and a variation, where the verification convention only calls for constant reality complexities at the price of an O(k)-measured open key. We also discuss some tradeoffs between different framework properties.

3. EXISTING SYSTEM AND ITS LIMITATIONS

The current cloud servers protect the data stored on the server by adhering to common cloud computing security primitives. As a result, the current cloud computing systems have the following drawbacks, for example:

LIMITATION OF PRIMITIVE SYSTEM

The following are the limitations of the existing system.

1. Information is only accessible via plain text, not encryption, in any of the existing systems. As a result, the data is not protected from unauthorised users connecting to the cloud server.
2. All of the existing cloud servers offer a standard plain text search capability, however they lack any secure search capabilities.
3. The cloud server won't ask any security primitive to obtain the data from the centralised server because it is stored in plain text.
4. Present-day cloud servers are virtually entirely managed centrally, allowing cloud service providers to watch and keep an eye on all access.
5. There is no such thing as a multi-layer solution for maintaining data privacy in a decentralised manner.
6. The current cloud servers were unable to recognise the value of fog computing in supplying data security.

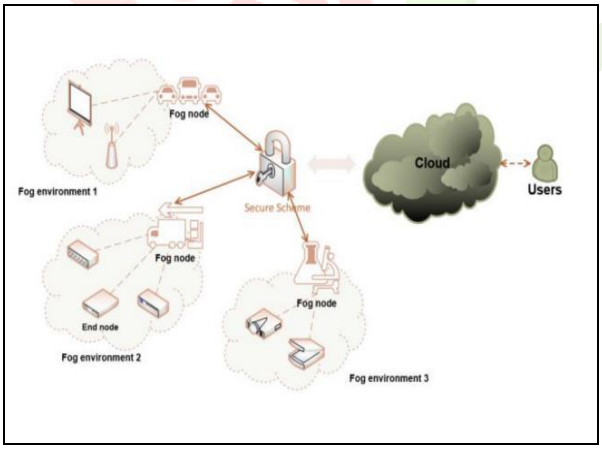
4. PROPOSED SYSTEM AND ITS ADVANTAGES

In the proposed thesis, we attempt to create a safe method SBBS where data may be partitioned into various portions and stored on a single fog node to store and access in a secure way utilising block chain encryption. Consequently, we can provide a system with more security.

ADVANTAGES OF THE PROPOSED SYSTEM

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.
5. In this proposed system we try to apply HMAC Algorithm for providing security of cloud data which is stored into the fog nodes.
6. In general the HMAC will provide data privacy as well as data integrity by generating hash key for the input text which is uploaded into the fog nodes.
7. If any un-authorized users try to modify or miss-use the data from fog server, immediately the cloud server can intimate to the data user with the help of hash code.

PROPOSED ARCHITECTURE



5. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes Php, HTML and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1. DATA OWNER MODULE

In this module, the data owner need to logs in by using his/her user name and password. After Login the owner Uploads Data, View Files Blocks.

2. DATA USER MODULE

In this module, he logs in by using his/her user name and password. After Login the user will do some operations such as Request Search Permission, Download Request, View All Files, and Download File.

3. FOG SERVER MODULE

In this module, the Fog Server can do following operations such as View Files Blocks, View All Fog User Details and process the end user operations to send data block.

4. CLOUD SERVER MODULE

The Cloud server as a server to provide data storage service and can also do the following operations such as View End Users and Authorize ,View Data Owners and Authorize, View All Stored Data, View Transactions ,View Attackers, View Search Request, View Download_Request,View Files Rank In Chart.

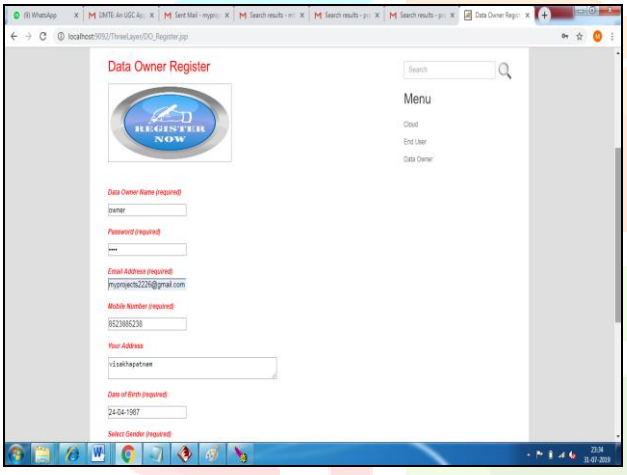
6. EXPERIMENTAL RESULTS

In this section we try to design our current model using PhP as programming language and taking MY-SQL as storage database. Here the front end of the application is designed using PhP and HTML and back end we used My-SQL server.Now we can check the performance of our proposed application as follows:

HOME PAGE

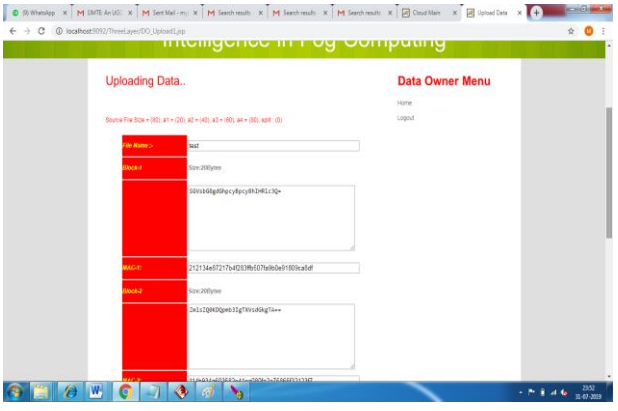
From the above window the user can see four modules in the main page.

REGISTRATION FORM



From the above window the user can see registration of user while he want to login into the account.

FILE UPLOAD MODULE

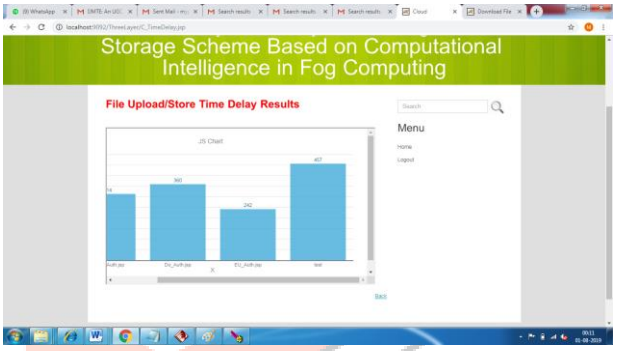


From the above window we can clearly see that owner will upload the file into the cloud server in an encrypted manner and he will divide the file into number of blocks.

UPLOAD CONFIRMATION PAGE

From the above window the user can see FILE is uploaded successfully into number of blocks.

TIME DELAY



From the above window the user can see FILE delay status in the form of chart.

7. CONCLUSION

In order to store and access the data from the cloud server in a safe way, we have for the first time in this work developed a Three Layer Approach. For the modern cloud, where data may be kept on several nodes rather than entirely on one storage media, we have integrated the Fog Server idea here. Here, we attempt to split the data into numerous blocks, each of which is encrypted by the owner of the data. In order to access a file, a user must first request it from a cloud server, which will attempt to provide access authorization for several blocks. If the cloud server grants access, the users may then view the file. Anyone without authorization from many levels must access the file in an encrypted way; they cannot view the contents in plain text. Our suggested protocol has undergone a number of studies, and the comparative results show that it is the best at ensuring the security of sensitive data

kept in server space.

8. 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,"Efficientdatacollection 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, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme 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.

[12]Fu,F.Huang,K.Ren,J.Weng,andC.Wang,"Privacy-preservingsmart semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

9. About the Authors

GUDIWAKA VIJAYALAKSHMI is currently working as an Assistant Professor in Department of Computer Science and Engineering at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh. She has more than 2 years of teaching experience. Her research interest includes Java, Python, .Net, HTML.

GARIKINA BHUVAN CHANDAR is currently pursuing his 2 years MCA in Department of Computer Science and Applications at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh.His area of interest includes C, C++, Java and Python.