INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 26th Apr 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue= Spl Issue 05

DOI: 10.48047/IJIEMR/V11/SPL ISSUE 05/03

Title **PRIVACY-PROTECTING CLOUD STORAGE SCHEME WITH THREE LAYERS BASED ON COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING**

Volume 11, SPL ISSUE 05, Pages: 16-22

Paper Authors

Ms.D.Rathna Kumari ,K.Asish, M.D.L Prasannai, L.Chinnari,I.Naveen

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

PRIVACY-PROTECTING CLOUD STORAGE SCHEME WITH THREE LAYERS BASED ON COMPUTATIONAL INTELLIGENCE IN FOG COMPUTING

Ms.D.Rathna Kumari[1] ,K.Asish[2], M.D.L Prasannai[3], L.Chinnari[4],I.Naveen[5]
Assistant Professor[5] Dept of CSE , B.Tech Students[1, 2, 3,4], Department of Computer Science Engineering, Ramachandra College of Engineering, Eluru, AP, India
dratna03.kumari@gmail.com , asish.konkimalla@gmail.com , lakshmiprasannamdbtech@gmail.com, chinnarilankapalli509@gmail.com , naveenroy732@gmail.com

Abstract—.Cloud computing technology has advanced significantly in recent years. Cloud storage technology is receiving greater attention and better development as unstructured data grows at an exponential rate. However, the present storage structure stores all of the consumer's data on cloud servers. In last words, consumers lose control over their data and suffer privacy breaches. Traditional privacy protection strategies rely on encryption technology, however these methods are unable to withstand an bout from inside a cloud server. We advise a three-layer storing structure built on fog computing to overcome this challenge. The proposed system may take complete advantage of cloud storage while still safeguarding data privacy. Furthermore, the Hash- Solomon code technique is projected to partition info into many units.

Keywords: Three Layer Storage Scheme, Fog Computing, Security, Privacy.

I Introduction

Computer technology has advanced significantly in the twenty-first century. Cloud computing is a new technology that was first introduced by San Jose in SES 2006 (Search Engine Strategies 2006) and defined by NIST (National Institute of Standards and Technology). Cloud computing is a expertise that allows data to be preserved, managed, and backed up regardless of where it is stored.

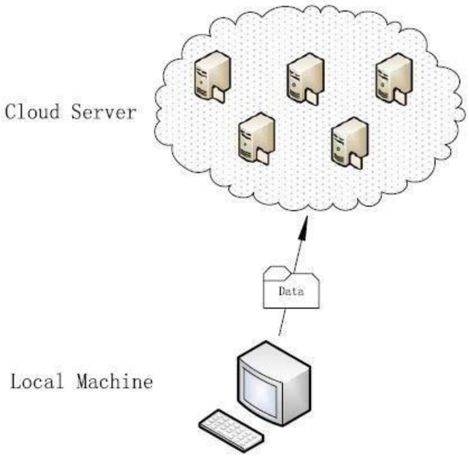
With the quick advancement the volume of customer information is increasing mathematically as a result of the organization's transmission capability. Consumer's necessity can't be satisfied by the boundary of nearby mechanism any longer. Thusly, folks effort to track down novel approaches for storing their data

A growing number of consumers are opting for distributed storage in order to increase their storage capacity. From now on, storing data on a public cloud server determination be the norm, and distributed storage innovation will flourish. Become far and wide in a twosome of years.

Distributed storage is a distributed computing platform that provides data capacity and management to executives. Distributed storage enables a large number of different stockpiling gadgets cooperate in a coordinated manner thanks to a variety of applications, network innovation, and disseminated record framework improvement. There are numerous organisations nowadays that provide a diversity of dispersed storage administrations, such as Dropbox, Google Drive, iCloud, Baidu Cloud, and so on. These organisations afford a large capacity and several administrations associated with other well-known apps, which aids their expansion in attracting diverting supporters. In any event, there are numerous security concerns with distributed storage administration. Among the security concerns, the subject of protection is particularly important.

For the most part, consumer transfers info to the cloud server directly. In this manner, the

Cloud Server Provider (CSP) determination occur consumer's ability to deal with the information As a result, clients have little control over the actual storage of their data, resulting in the division of custody and the management of data. The CSP has unrestricted access to and searches of the data stored in the cloud. In the meantime, attackers can attack the CSP server to obtain the client's information. Both of the above situations expose consumers to the danger of data leakage and information loss. Typical secure distributed storage solutions for the aforementioned concerns focus on access restrictions.



Regardless of how the calculation is done, these arrangements can't handle the inside attack well gets to the next level. In this way, we suggest a Three Layer Storage(TLS) conspire in light of fog supposing model and plan a Hash-Solomon code in view of Computational Intelligence.

Haze processing is a lengthy figuring model in view of a mist hub is a type of distributed computing that consists of a large number of mist hubs. These hubs have a certain amount of storing and handling capabilities.

We divided the client's information into three sections in our strategy and saved each section separately in the cloud server, the haze server, and the client's nearby PC. Furthermore, based on the Hash-Solomon code's property, the plan may guarantee that fractional information cannot recover the initial information. Using Hash-Solomon code, on the other hand, will supply a portion of the surplus information blocks that will be used in the unravelling system. Increasing the number of repeating blocks not only improves the consistency of the stockpiling, but it also adds to the amount of data stored. Our plan may truly ensure the security of our clients' information by judicious information distribution. Complex estimate is required by the Hash-Solomon code, which can be aided by Computational Intelligence (CI).

Contrasted and conventional techniques, our strategy canister give a advanced security insurance after inside, mainly from the CSPs.

The respite of this paper is coordinated as trails: Section II reviews related research effort, Section III nitty gritty expounds the TLS manufacturing, the Enactment detail of work procedure, the proposed security examination of the stockpiling plan and the output investigation suggested in this paper, Section IV measures the plan by numerous tests and Section V appearances up this paper in conclusion.

II Procedure

Put away Procedure: When consumer needs to store his text to the cloud server, the system is by way of follows :

As a matter of some importance, consumer's record determination be prearranged with Hash-Solomon code. Then afterward, the record will be broken down into a few data blocks, and the framework will also be critical of data encoding. It's expected that 1% of information blocks and encoding data will be stored locally. The remainder of the data blocks will be sent to the mist server.

Also, in the awaken of getting the almost 100% info blocks from consumer's machine, these info blocks will be prearranged with Hash-Solomon in the future. These info blocks will be remote into more modest info obstructs and produces novel programming data. Additionally, expecting that 4% info blocks of the data for encoding will be stored on the mist server. The remaining data blocks will be uploaded to the cloud server.

Thirdly, afterwards cloud server got the info blocks structure cloud side, these info blocks will be appropriated by cloud supervise framework. At extended last, the volume methodology reaches once all the connected info be kept in numerous servers.

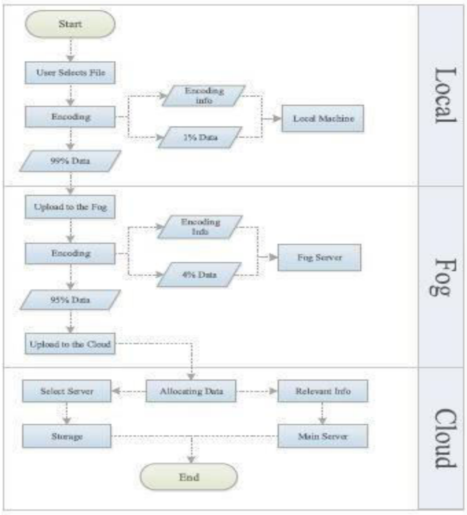


Fig. 3. Diagram of stored procedure.

2) Download Procedure: Once client needs to transfer his record from the cloud server, methodology is as follows:

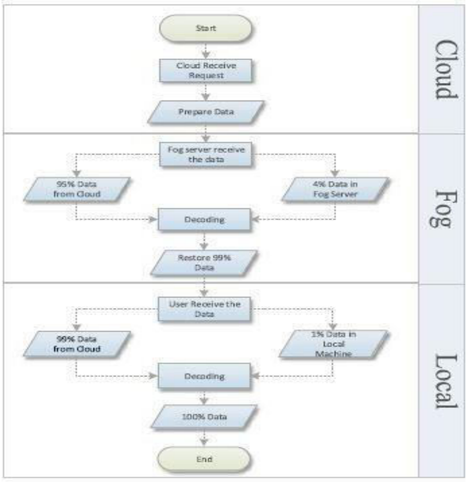


Fig 4. Diagram for downloading procedure

Cloud server, right off the bat, accepts consumer's solicitation then afterward coordinates the data in numerous appropriated servers. Afterward joining, cloud server directs the 95% data to the mist server.

Furthermore, the mist over server gets the data as of the cloud server. Joining by the 4% data blocks of mist server and the programming data, we can recuperate almost 100% information. Then the haze server returns the 9% data to the client. With the quick advancement the volume of customer information is increasing mathematically as a result of the organization's transmission capability. Consumer's necessity can't be satisfied by the boundary of nearby mechanism any longer. Distributed storage enables a large number of different stockpiling gadgets cooperate in a coordinated manner thanks to a variety of applications, network innovation, and disseminated record framework improvement.

Finally, the client receives data from the hazy server. By rehashing the above developments, the client can obtain all of the information.

III Related Work

The implication of safety in scattered storage needs drawn in a heap of thought regardless of in academe or industry. Here are a ton of explores around secure distributed storage designs lately. Shen et al. contemplate cloud is semi-trusted and suggest a structure for metropolitan data sharing by taking advantage of the individual based cryptography. The strategy they proposed is secure and can oppose potential attacks.

When a consumer requests information from a cloud server, the client provides the server a secret key for identification. In the event that the secret phrase is discovered, the design employs a topsy-turvy reaction mode. Hou, Wu, Zhen and Yang call attention to that the safe center of distributed storage is safety and protection in appropriated framework. Consequently they propose a safe computer-generated insurance plot in light of SSL. By moving information over SSL and conveying happening the cloud server, the framework scrambles information beforehand it is composed hooked on the hard plate.

Notwithstanding, these encryptions make search in cloud more troublesome. Presently, accessible encryption is a hotly debated issue in the field of distributed computing. Every one of them accomplishes high precision, security and effective. Shen Wei et al. bring up that the majority of the past works on the cloud security center around the capacity security instead of thinking about the calculation security together. Atan R et al. propose a safe structure, comprising of two fundamental layers: specialist layer and cloud information capacity layer. The design incorporates five sorts of specialists: User Interface Agent, User Agent, DER Agent, Data Retrieval Agent and Data Distribution Preparation Agent. The explores above are enhancements of security assurance in distributed storage in various perspectives.

Some of them use assortment encryption strategies in various positions. Others take care of the protection issue with the assistance of examining or constructing their own safe structure. Nonetheless, there is a typical imperfection in these explores. When the CSP is untrusted, these plans are invalid. Subsequently, In this study, we offer a new safe distributed storage layout. We may provide serious degree security assurance of information by partitioning records with explicit code and combining with TLS structure in light of haze processing model.
This isn't to say that we're abandoning encryption research. Encryption also aids us in safeguarding fine-grained information security in our strategy.

Cloud computing technology has advanced significantly in recent years. Cloud storage technology is receiving greater attention and better development as unstructured data grows at an exponential rate. However, the present storage structure stores all of the consumer's data on cloud servers. In last words, consumers lose control over their data and suffer privacy breaches. Traditional privacy protection strategies rely on encryption technology, however these methods are unable to withstand an bout from inside a cloud server. We advise a three-layer storing structure built on fog computing to overcome this challenge. The proposed system may take complete advantage of cloud storage while still safeguarding data privacy. Furthermore, the Hash- Solomon code technique is projected to partition info into many units.

IV Secure Cloud Storage Based on Fog Computing

The security degree is an important metric for determining the nature of a distributed storage system. Furthermore, information security is the most important aspect of distributed storage security, and it encompasses three perspectives: data protection, data respectability, and data accessibility.

Guaranteeing data security and honesty has forever remained the focal point of pertinent investigates. On another hand, info security is moreover the greatest concerned piece of the consumers. According to a business belvedere, society with high security notch will attraction in additional clients. Accordingly further developing security is an essential impartial irrespective of in scholarly biosphere or commercial.

A Fog Computing

Cloud computing technology has advanced significantly in recent years. Cloud storage technology is receiving greater attention and better development as unstructured data grows at an exponential rate. However, the present storage structure stores all of the consumer's data on cloud servers. In last words, consumers lose control over their data and suffer privacy breaches. Traditional privacy protection strategies rely on encryption technology, however these methods are unable to withstand an bout from inside a cloud server. We advise a three-layer storing structure built on fog computing to overcome this challenge. The proposed system may take complete advantage of cloud storage while still safeguarding data privacy. Furthermore, the Hash- Solomon code technique is projected to partition info into many units.
Our plan depends on haze figuring model, which is an augmentation of distributed

computing. Haze registering was proposed by Ciscos Bonomi, right off the bat, in 2011. Contrasted with exceptionally focused distributed computing, haze processing is nearer to edge organization and enjoys many benefits as follows: more extensive geological disseminations, higher constant and low-inertness. In considering of these characters, haze figuring is more reasonable to the applications which are delicate to delay. On another hand, contrasted with sensor hubs, mist registering hubs have a specific stockpiling limit and information handling capacity, which can do a few straightforward information handling, particularly those applications in light of geological area. Hence we can convey CI on the mist server to do a few computing works. Haze processing is a lengthy figuring model in view of a mist hub is a type of distributed computing that consists of a large number of mist hubs. These hubs have a certain amount of storing and handling capabilities. The focus of this topic is on information storage and security. When a record is transferred to the cloud by the owner, the document's intricacies are visible in the cloud. Cloud can also see client demand details as well as record download history. We plan client functionalities in this module. The client can view the records that are available and submit a request for document delivery. The customer can fully download the document after receiving the key from the information owner.

Haze figuring is characteristically a three-level engineering, the maximum is distributed computing layer which has strong capacity limit and process capacity. A higher level is mist registering layer. Besides, we strategy a serviceable exhaustive productivity record, to achieve the greatest proficiency. Similarly broadening our work by carrying out a model which will uphold genuine execution of haze based web of things. The haze figuring layer fills in as the center layer of the haze registering model and assumes a pivotal part in transmission between distributed computing layer and sensor network layer. The mist hubs in haze registering layer has a specific stockpiling limit and figure capacity. The base is client's neighborhood machine. The principal work of this layer is gathering information and transferring the information to cloud server. Furthermore, the exchange rate between mist registering layer and different layers is quicker than the rate straightforwardly between cloud layer and the base layer. The presentation of haze figuring can alleviation the distributed computing layer, further developing the work productivity. In our plan, we exploit the haze registering model, embrace three-layer structure.

B Three-Layer Privacy Preserving Cloud Storage Scheme Based on Fog Computing Model

To safeguard client's security, we propose a Three Layer Storage system in light of haze processing model. The TLS system can provide client with a specific force of the executives and really safeguards client's protection.

The internal assault, as previously stated, is difficult to resist. When it comes to dealing with outside threats, traditional methods are effective, but when it comes to dealing with difficulties within CSP, they are ineffective.
Unlike traditional approaches, our strategy divides the client's data into three different-size leaves behind encoding innovation. Every single one of them will miss the mark on a crucial piece of classification data. In line with the haze registering model, the three pieces of data will be stored in the cloud server, the haze server, and the client's nearby machine, depending on the request size. The attacker cannot recover the client's unique information using this approach, even if he obtains all of the information from a single server. Because both the haze server and the nearby machine are bound by clients, the CSP can't receive any useful data without the information stored in the haze server and nearby machine.

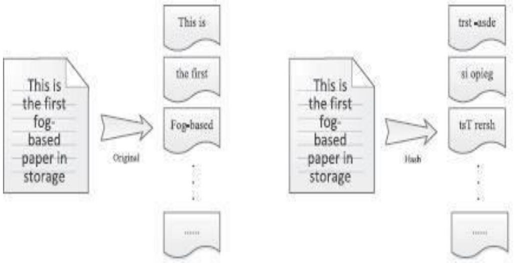

This is the first fog-based paper in storage
Original
This is
the first
Fog-based
......
This is the first fog-based paper in storage
Hash
trst -asdc
si opieg
tsT rersh
......

Fig. 3. Original transform vs. Hash Transform

As displayed in Fig. 2, the TLS system takes full advantage of haze server's stockpiling and data handling capacity. Every server saves a exact piece of info; the volume still up in the air by client's designation technique. Client's information, first and foremost, will be encoded on the client's local computer Then, for example, inject 1 percent encoded information into the system at that point. After that, send the rest of the data to the hazy server. In addition, we perform comparing actions on the hazy server with data from the client's workstation. Around 4% of the data will be stored on the mist server, with the balance being sent to the cloud server later.

The overhead activities be contingent on Hash-Solomon code. Hash-Solomon code is a sort of coding approaches in view of Reed-Solomon code. In the wake of existence encoded by Hash-Solomon code, the information determination be isolated into k parts and creates m excess information. Hash-Solomon code has such possessions, in these k+m parts of information, assuming somebody has essentially k parts, he can recuperate the total information. In other word, It is impossible for anyone to recover the entire data set with less than k pieces of data.As a result, we can ensure that the information of our clients is secure. The internal assault, as previously stated, is difficult to resist. When it comes to dealing with outside threats, traditional methods are effective, but when it comes to dealing with difficulties within CSP, they are ineffective.

Plus, the haze because each hub in the mist server has its own calculating power, the server includes Computational Intelligence, which can assist the framework in determining the ramifications of the upsides of k and m.

C Theoretical Safety Analysis

This unit will present a theoretic safety examination of the arrangement planned in our study and demonstrate that the secure storing structure can significantly increase privacy protection capability. With slightly single server's data, recovering the original data is impossible. The TLS framework largely eliminates user privacy leaks.

As displayed in above figure, the primary code divides a sentence into different portions in a specific order. Regardless, the hash code divides the statement into several pieces based on arbitrary organisation. As a result, Hash-Solomon code improves security assurance and prevents the adversary from obtaining fragmented data. Then the haze server returns the 9% data to the client. With the quick advancement the volume of customer information is increasing mathematically as a result of the organization's transmission capability. Consumer's necessity can't be satisfied by the boundary of nearby mechanism any longer. Distributed storage enables a large number of different stockpiling gadgets cooperate in a coordinated manner thanks to a variety of applications, network innovation, and disseminated record framework improvement.

Finally, the client receives data from the hazy server. By rehashing the above developments, the client can obtain all of the information.

V Modules

Our Project consists of the following modules :

- Owner
- Fog server
- Cloud
- User

Modules Description:

Owner Module: We develop the Owner functionalities in the primary module. In the Owner module, the proprietor can transfer another File and register document isolated with blocks and saves in three places with MAC code.

Fog Server Module: Owners can verify the record details and document download history in the Fog Module. On the same way as the cloud does, in the haze server, some information will be set aside for security reasons. If the entire document needs to be accessed, the Fog server stores information that is also required for complete access to the record; but, with our partial information, the entire record cannot be accessed. As a result, the document download history will also be available in the Fog module.

Cloud Module: The focus of this topic is on information storage and security. When a record is transferred to the cloud by the owner, the document's intricacies are visible in the cloud. Cloud can also see client demand details as well as record download history.

User Module: We plan client functionalities in this module. The client can view the records that are available and submit a request for document delivery. The customer can fully download the document after receiving the key from the information owner.

VI Conclusion

The progression of distributed computing provides us with numerous benefits. Distributed storage is a useful innovation that allows customers to increase their capacity limit. Distributed storage, on the other hand, brings forth a slew of security difficulties. When clients use dispersed storage, they lose control over the actual storage of their data, resulting in the parting of possession and the board of information. To address the issue of dispersed storage security, we offer a TLS structure based on a hazy figuring model and a Hash-Solomon computation. The plan turned out to be feasible after the hypothetical security investigation.

By distributing We can safeguard the security of info in individually server by balancing the quantity of information blocks stored in multiple servers. On the other side, theoretically, contravention the encoding network is unfathomable. In addition, to hash change to protect fragmented data is a good idea.During the trial, this plan successfully completed encoding and decoding without affecting circulated storage productivity.

Besides, strategy a serviceable exhaustive productivity record, to achieve the greatest proficiency. Similarly broadening our work by carrying out a model which will uphold genuine execution of haze based web of things.

VII. 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 cloud computing environments,” in *Proc. IEEE Int. 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] Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, “Efficient data collection 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.