International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217135

Data Protection for Files and Logs in Fog Cloud Storage Using 3DES

D. Vannur Vali
M. Tech Scholar, Department of CSE, JNTUA, Ananthapuramu, Andhra Pradesh, India

Article Info
Volume 7, Issue 1
Page Number: 174-181
Publication Issue :
January-February-2021

Article History
Accepted : 01 Feb 2021
Published : 08 Feb 2021

ABSTRACT

Nowadays cloud computing is being used extensively in daily life. With these new computing and communication technologies, new data security challenges arise. Privacy, integrity, and availability are the primary goals of the security structure. Many authentication schemes have been introduced over the years to ensure better security and to provide a wider range of services with a faster perspective. Each type of data is stored in the cloud and can be easily accessed anytime, anywhere. But, it lags due to location awareness when it comes to privacy in cloud computing. Improved cloud computing uses a fog-centric secure plan to ensure logs and information against unapproved access, change, and extinction. To obstruct unauthorized entry, the current scheme uses a technology called Xor-Combination to hide data. Besides, Xor-Combination results in preventing malicious recovery and ensuring better recovery capacity in case of data loss and Intermediate Fog does not provide server security. Cloud server and log files have been proposed and improved to provide higher security and intermediate security differently compared to the existing system for storing data on the fog server. Log files also contain personal information with equally critical protection and confidentiality of log data as an alternative scheme for storing logs in a cloud environment. Our proposed security to protect log files and data files on the main server on the Intermediate Fog server. We use an enhanced 3DES security method that provides better security than the Xor-combination technique.

Keywords : Cloud Storage, Fog Security, 3DES Technique, Log Files, Cloud Service Provider.

I. INTRODUCTION

Emerging technologies such as Cloud Computing use central architecture to make available different resource usage. In today's technology, cloud service providers provide highly obtainable storage along with especially comparable computing reserves at similarly low expenses. As a low cost and efficient technology, data storage and use of different specified privileges has increased dramatically. In this cloud storage service, the most critical problem is the always expanding amount of information and control of data storage duplication. Data de-duplication for copy duplicates of information away is a particular information durability strategy.

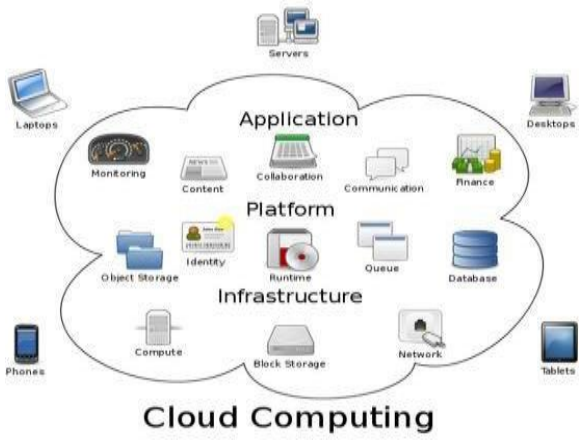

Fig 1: Cloud Architecture

In the customary cloud computing situation, when clients re-appropriate their information to the cloud, they can't secure it actually. CSP can browse, scan or change cloud-saved data. Simultaneously, the Service Provider may lose the information accidentally because of some specialized issues. Alternatively, an attacker can abuse the protection of the client information. Utilizing some cryptographic systems, (for example, encryption), secrecy or trustworthiness can be ensured. Nonetheless, the cryptographic methodology can't forestall inward assaults, regardless of how much the calculation improves. To ensure information secrecy, trustworthiness and accessibility a few examination networks presented Fog Computing setting mist gadgets in the middle of the client and the cloud.

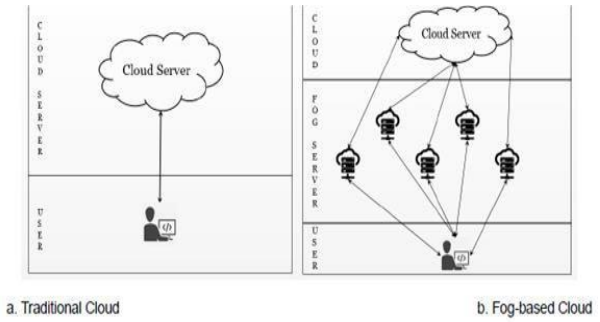

Fig 2: Existing Architecture

In the conventional cloud computing domain, the cloud worker bolsters the client with calculation, stockpiling, and systems administration offices. In this situation, a client straightforwardly transfers their information either for care or for preparing with adaptable figuring/stockpiling assets which is delineated in Figure. 2. In any case, re-appropriating information to the cloud may penetrate the protection of the information. Moreover, there are circumstances where a lot of information gets amassed from a specific area and is handled continuously to create some outcome. Sending information to a brought together framework (for example cloud worker) may cause transmission delays. Haze figuring can resolve this issue. Mist figuring is a more modest form of distributed computing that is placed between the cloud worker and the client. Fig. 2 shows the situation of a haze based distributed storage framework. As the client needs the reliable capacity to save information, the proposed plot considers engineering where the client has full command over mist gadgets. Clients can depend on mist figuring/stockpiling gadgets for the administration of their information. In the existing architecture, the author uses security only for data files in the main server and lesser security concept Xor combination algorithm. An existing secure cloud storage scheme based on fog computing employing Xor-Combination, Block Management, and CRH operation. Xor-Combination together with Block Management contributes to maintaining the privacy and preventing data loss. CRH ensures the discovery of information change. Hypothetical security examination demonstrates the protection ensures Log Security, information recoverability, and change the recognition of the proposed conspires. The framework actualized a model variant of the plan and directed trials to check its exhibition in correlation with the contemporary plan. Results demonstrate its effectiveness as far as time and memory utilization. The paper's main contributions can be summarised as below:

We proposed a protected cloud storage program dependent on fog computing utilizing data and log security using 3des.

Supposed security examination demonstrates the protection ensure, information recoverability, and change location of the proposed conspire.

We actualized a model adaptation of the plan and directed tests to check its presentation in examination with the contemporary plan. Results demonstrate its proficiency regarding time and memory utilization.

II. RELATED WORK

The long-dreamed vision of computing as a resource is cloud computing, Users can conveniently access their data in the cloud and achieve excellent on-demand software and services from a common network of configurable computing resources. By means of data sharing, users can be relieved of the burden of local data storage and maintenance. The idea that users no longer have physical possession of the potentially wide scale of outsourced data makes it a very challenging and potentially overwhelming challenge to maintain data privacy in Cloud Computing, especially for users with restricted computing capacities and resources Therefore, allowing public audit capability for cloud data storage security is of essential significance so that consumers can use an external audit group to check the quality of outsourced data when appropriate.The following two fundamental criteria must be fulfilled in order to securely implement an effective third-party auditor (TPA): 1) TPA should be able to inspect cloud data storage efficiently, without having local data replication, and not place any extra online pressure on the cloud customer.2) The third-party auditing process does not add any additional threats to consumer data privacy. In this article, the public key-based homomorphic authenticator is used and uniquely paired with random masking to accomplish a public cloud data auditing scheme that protects privacy, which meets all of the above criteria. We further investigate the bilinear aggregate signature methodology to extend our key finding into a multi-user environment to promote the successful management of multiple auditing tasks, where TPA will execute multiple auditing tasks at the same time. Comprehensive tests of protection and efficiency demonstrate that the proposed schemes are proven to be secure and highly efficient.

L. Xiao et, al., [7] The main problem in the age of cloud computing is the security of data and user data privacy. Due to limited security for data owners, the appropriateness and privacy of data stored in the cloud could be affected. This paper provides a comprehensive survey on cloud computing issues related to privacy preservation, data and storage security.The Cloud data protection is further analysed in terms of the confidentiality of data, access management and attribute-based encryption. In depth, the survey analyzes each sort of work. A comparison table along with the strengths and disadvantages of each strategy is also presented.

J. Hou and T. Fan, [8], We propose a novel protection safeguarding security answer for cloud administrations. Our answer depends on a productive non-bilinear gathering mark conspire giving unknown admittance to cloud benefits and shared stockpiling workers. The epic arrangement offers unknown validation for enrolled clients. Hence, clients' ascribes (age, legitimate enrollment, fruitful installment) can be demonstrated without uncovering clients' personality, and clients can utilize cloud administrations with no danger of profiling their conduct. Nonetheless, if a client disrupts the supplier's norms, his entrance right is disavowed. Our answer gives unknown access, unlikability, and the privacy of sent information. We actualize our answer as a proof of idea application and present the trial results. Further, we investigate current protection saving answers for cloud administrations and gathering mark plans as essential pieces of security improving arrangements in cloud administrations.

We contrast the exhibition of our answer and the connected arrangements and plans.

G. Feng, [9] As of now, there is a great deal of developing encryption instruments and access control models for the assurance of the information contained in the cloud climate. Notwithstanding, the examination on the security insurance of information credits in the cloud is as yet in the underlying stage, which can be ordered into two kinds: one is the privacy assurance of information ascribes during information transmission, including directing data, age time, size, and recurrence, and so on, the other is the protection assurance of information credits as information stockpiling, including connections among traits and dissemination of quality qualities. The current encryption systems and access control models can't take care of the issue impeccably. In this paper, we attempt to investigate momentum security plans and calculations for the insurance of information credits and point out future exploration bearings.

Z. Xia, and Q. Wang, [10] Increasingly more information proprietors are roused to re-appropriate their information to cloud workers for incredible accommodation and diminished costs in managing the information because of the rising popularity of cloud computing.However, prior to outsourcing for privacy requirements, Confidential information that outdates data use, such as keyword-based database extraction, should be encrypted. In this paper, we introduce a protected multi-keyword confidential search system over encrypted cloud data, which also facilitates dynamic update operations such as deletion and insertion of documents.Particularly, in index construction and query generation, the vector space model and the commonly used TF x IDF model are combined. In order to provide a successful multi-keyword ranked search, we construct a unique tree-based index structure and propose a "Greedy Depth-first Search" algorithm. To encrypt the index and query vectors, the secure KNN algorithm is used, thus ensuring accurate calculation of the relevance score between the encrypted index and query vectors. Phantom terms for blinding search results are applied to the index vector to resist statistical assaults. Because of the use of our unique tree-based index layout, the suggested method will achieve sub-linear search time and cope with the deletion and inclusion of documents flexibly.

In order to show the effectiveness of the proposed system, extensive evaluations are carried out.

III. PROPOSED APPROACH

Output-highly utility technologies have been explored in many cases to increase security on intermediate servers and major servers. Work on the current machine considers the difficulty in setting security levels for the intermediate server, which is a concept that is challenging for fog servers and so far there is no such concept of enforcing fog log security. The authors of the proposed machine use the entropy maximization framework to increase the new output-highly desirable security levels on cloud servers. The proposed work is a different approach compared to the existing system for storing data in the cloud using segment technology and fast multipath routing. The improved approach provides better efficiency and security for cloud storage and fog operations.

This system is designed to build cryptographic protocols to solve problems of integrity and privacy as log records are stored, preserved, and queried, and to improve the reliability of the Fog server.Cloud security is a very important part of data security because it is transmitted through networked computers it is responsible for securing all information. Cloud Security All Hardware and Software Functions, Features, Functionality, Policies, Accountability, Measurements, Access Control and Acceptable for Hardware and Software indicates the

administrative and management policy and information in the network needed to provide protection. Cloud security issues can be divided into about four related areas: privacy, authentication, denial, and Integrity control. The secret, also known as privacy, is to keep information out of the unauthorized hand's Customers. When people think of network security, this commonly comes to mind.To disclose sensitive information or to enter into a business agreement Authentication performs the determination ofwho you are talking to before logging in. We have the log file architecture as shown in Fig. 3

Improving, which provides security for query log records on the intermediate server and data security for the cloud servers.

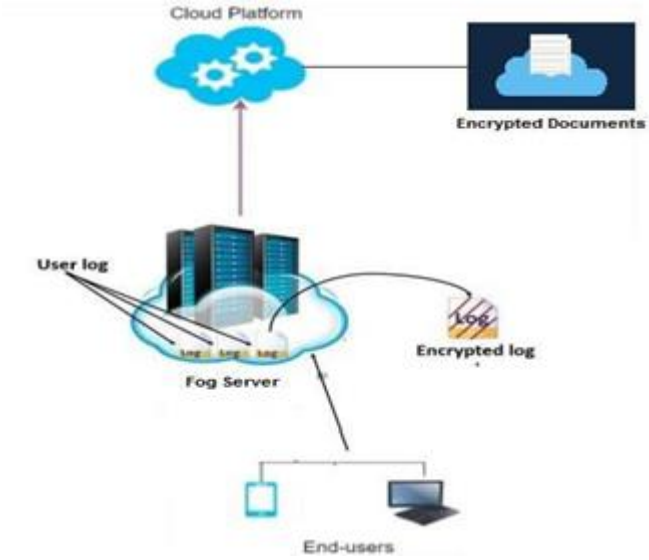

Fig 3: Fog Cloud Architecture with Logs andData Security

Privacy, integrity, and availability are the primary goals of the security structure. To ensure that several standardization schemes are introduced over many years. Currently, the expansion of private key infrastructure is a very important solution. PKI, which contains the conversion key using authentication documents through the public channel to authenticate users in the cloud infrastructure. This paper aims to examine the existing basic security structure and this further new proposed security structure Seeks to introduce, furthering the knowledge of 3DES mechanics and current progress in research in 3DES computing utilizes to provide a secure structure. The Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cypher that applies the DES cypher algorithm three times to each data block. The 56-bit Data Encryption Standards (DES) key is consistent with current methods of cryptography research and supercomputing ability.

Algorithmic View

Begin

1: for each session separated for every user does

2: Get different HTTP requests and activities of the user (DB queries q, Storage S, Services r) in this session

3: for each different r do

4: Add user Request to Log File with sessions (UserID, Db Query, Storage, Services)

5: if r is not in set USER login then

6: exit else

7: Encrypt Log File Activity(Db Query, Storage, Services)Encipher (String s, String key) for I = 0 to s.length() do char enciphered = s.charAt(i) + getShift(key,i) > 90 ? (char)((s.charAt(i) + getShift(key, i)) -26) : (char)(s.charAt(i) + getShift(key, i)) log.append(enciphered);

next

8: Append session ID with Log Activity

9: decrypt (String s, String key)For I = 1 to s.length() do char decyphered = s.charAt(i) - getShift(key, i)< 65 ? (char)((s.charAt(i) - getShift(key, i)) +26) : (char)(s.charAt(i) - getShift(key, i)); log.append(decyphered);

10: End

System Module:

In the realm of conventional cloud computing, the cloud worker bolsters the client with processing, storage, and systems administration facilities. In this

situation, the client transfers their information straight forwardly to get or handle it with adaptable registering/stockpiling assets, this is represented in figure2. Notwithstanding, re-appropriating information to the cloud may encroach on the security of the information. In any case, there are greater conditions all information is put away from a particular area and handled progressively to give a few outcomes. Sending information to a concentrated foundation (for example cloud worker) can cause transmission delays. Fog computing can tackle this issue. Haze figuring is a more modest variant of distributed computing that is set between the cloud worker and the client. Fig.2 shows an outline of a fog based distributed storage framework. Since the client needs the dependable capacity to save the information, the proposed plot considers the design where the client has full oversight over the mist gadgets. Clients can depend on mist figuring/stockpiling gadgets for their information on the board.

User Module:

User data module, the ultimate goal of this paper is privacy, disaster recovery, and editing of user data.

Fog Server:

Fog Server is user trusted. The client depends on the fog server with his information. The nearness of fog gadgets to the client, strong actual security, appropriate confirmation, secure correspondence, discovery of interruptions guarantee the fidelity of the fog server to the user.

Cloud Server:

The cloud server is considered to be a huge storage server. This suggests that the cloud server specifically fits the SLA, but is meant to interpret user knowledge. The cloud server, by comparison, pretends to be good but potentially works.

IV. RESULTS

A set of experiments will be conducted on social media users on stress-analysis data obtained from Facebook. The performance evaluation of the system is done by using its dataset. This section represents a comparison of the proposed scheme with the prior work of Wang et al. To make a logical comparison, we tried to align various factors such as environmental size, block size, correspondence speed, etc.

Data Processing

Selecting files ranging from 100KB to 1MB in each step, the pad was adequate to process using 2/3-Xor-Combination and the well-known Reed-Solomon code RS (255, 223). The partition function is the same for both schemes, so split comparison is avoided here. The experiment considers each data block, uses suitable algorithms to process it, and writes the time of execution. The data block methodology applies the metadata as seen in the table below to the client and cloud server database tables of the fog server.

Data/ Document ID	Block Tag	Cloud Server	File Size
1093	B14	Drive HQ	100
1094	B15	Drive HQ	200
1095	B16	Drive HQ	300
1096	B17	Drive HQ	400

Data Block Transmission

A table showing the upload ID of various documents of different sizes to run the HQ cloud with a block tag ID. These documents are transferred to drive the HQ cloud using the 3DES Intermediate Fog Layer Log Concept for greater security and log activity recorder. This shows that it is three-dimensional and faster than the Xor-Combination RS (255, 223). This is because only Xor computation is required by the

Xor-combination. The processor calculates directly inside its circuit. Reed-Solomon codes in the programme, by contrast, require the arithmetic operation of the Galois field and are not explicitly supported by a general purpose processor.For example, to run the Galois field multiplier in software, 0, two log table look-ups, one test for the module add, and anti-log table look-up are required.

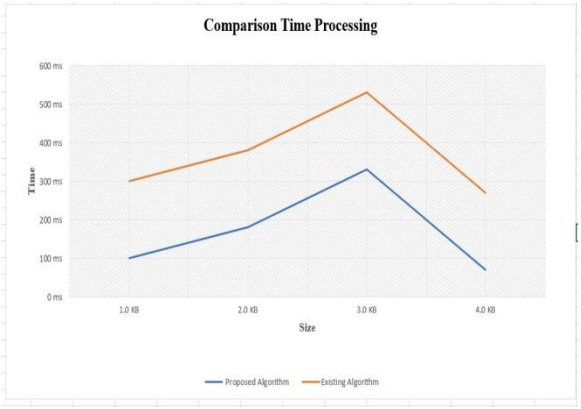

Fig 4: Uploading time (milliseconds) comparison using payload size in (KB)

Fig. 4 shows a comparison of the difference between the proposed (3DES) and the existing (Shaw) algorithm and the graph, showing that the proposed algorithm takes less time compared to the current algorithm. Here the time is measured in milliseconds (Y-axis)and size is shown in KB (X-axis). In fact, the current system has some benefits in the case of uploading a record from the cloud server to the fog server. For example, in the best-case situation where there is no malicious editing and/or data leakage, a portion of all composite blocks must be transferred from the cloud to the Fog server.However, in the event of malicious editing or data loss, all-composite blocks of the Fog server file will need to be downloaded increasingly.

V. CONCLUSION

Cloud computing tends to significantly transform the way we use computers to view and store our personal and business records. With these modern computing and communication systems, log security is enhanced on fog servers, new data security challenges arise. This paper demonstrates a novel security scheme that authenticates proof of secure storage of confidential data when deployed by fog-centric cloud storage architecture. This study provides an advanced computational security mechanism that solves the problem of internal nodes using effective security algorithms by reducing computational overhead.

The proposed approach increases FoG server capacity when processing data. Furthermore, it reduces the network bandwidth usage along with the dynamic updating of the data. Furthermore, this mechanism can be improved by taking into account the functionality of the edge network.

VI. REFERENCES

[1]. J. Shen, D. Liu, J. Shen, Q. Liu, X. Sun, A secure cloud-assisted urban data sharing framework for ubiquitous cities, Pervasive mobile-Computing(2017),http://dx.doi.org/10.1016/j. pmcj.2017.3.013

[2]. Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., & Zhang, Z.(2018). Secure Data Storage and Searching for IndustrialIoT by Integrating Fog Computing and Cloud Computing.IEEE Transactions on Industrial Informatics, 1–1.doi:10.1109/tii.2018.2793350

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

[4]. 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.

[5]. J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in a software-defined network(Sdn)

and cloud computing environments," in Proc. IEEE Int. Conf. Commun.,2014, pp. 2969–2974.

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

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

[8]. J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.

[9]. G. Feng, "A data privacy protection scheme of cloud storage," vol. 14, no. 12, pp. 174–176, 2015.

[10].Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distribution System., vol. 27, no. 2, pp. 340–352, Feb. 2016.

Cite this article as :

D. Vannur Vali, "Data Protection for Files and Logs in Fog Cloud Storage Using 3DES", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 1, pp. 174-181, January-February 2021. Available at doi : https://doi.org/10.32628/CSEIT217135
Journal URL : http://ijsrcseit.com/CSEIT217135