Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 14s (2025)
https://www.jneonatalsurg.com

Resilient Data Protection in Fog-Cloud Environments Using Fragmentation and Advanced Cryptography

[1*] Yuvana Tagore, [2] R.Vijaya Kumar Reddy, [3] Dr.T.Vengatesh

[1*]Department of CSE, Koneru Lakshmaiah Education Foundation,Vaddeswaram ,Andhra Pradesh, India

[2]Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.

[3]Assistant Professor, Department of Computer Science, Government Arts and Science College, Veerapandi, Theni, Tamil Nadu, India.

[2] rvijayakumarreddy@kluniversity.in,

[3]venkibiotinix@gmail.com

[1*]**Corresponding Author:** tagoreyuvana@gmail.com,

.Cite this paper as: Yuvana Tagore, R.Vijaya Kumar Reddy, Dr.T.Vengatesh, (2025) Resilient Data Protection in Fog-Cloud Environments Using Fragmentation and Advanced Cryptography. *Journal of Neonatal Surgery*, 14 (14s), 33-38.

ABSTRACT

Unless users use a cloud storage service for their sensitive data, the storage service is excellent. Once data is outsourced to the cloud, the cloud server has complete access to and control over the user's data. It can have the capacity to read and search user data. Emerging cyber threats to cloud storage include data loss, malicious modification, and privacy invasion. Fog server-based three-layer architecture for safe storage has just been introduced. According to the design, some data will be saved on the user's local system, in the cloud, and fog. A fraction of the data in the cloud and their unique hash method require additional processing and storage. An approach to cloud storage based on fog is used in this study. In that technique, data is divided into many blocks using the XOR operator, and these multiple blocks are then combined into two or three blocks. As a result, we increase the security of the fog server for a resilient fog-centric cloud computing architecture and we improve the cryptosystem to secure data without revealing any information from it using this technique. Data is protected from unauthorised access, modification, and deletion via the fog-centrioud storage system.

Keywords: *Cloud computing, Servers, Secure Storage, Privacy, Xor-Combination*

1. INTRODUCTION

When using traditional cloud computing, customers can no longer physically protect their data once they have moved it to the cloud. A cloud service provider (CSP) can access, browse, or edit the data that is stored there. Additionally, due to a few technological issues, the CSP could unintentionally lose some data. Alternately, a hacker could compromise the user data's privacy. Confidentiality or integrity can be protected using some cryptographic processes (such as encryption, and hash chains). No matter how much the method is improved, internal attacks cannot be prevented by a cryptographic approach. Several research communities introduced the concept of fog computing, inserting fog devices between the user and the cloud server to safeguard data confidentiality, integrity, and availability (CIA). The suggested system is a fog computing-based secure cloud storage solution. To increase the secure data search's effectiveness in fog-based cloud services. Effective data usage services are difficult to provide because sensitive data from end users must be encrypted before being sent to the fog node to ensure data privacy. Searching for keywords within encrypted data files is one of the most crucial services. The proposed approach is the first ever to allow concealed queries, query isolation, controlled searching, and proved secrecy for encryption on encrypted data. The ability for cloud servers to calculate cryptic data without disclosing any information, and to enhance the security of fog servers for a solid fog-centric cloud computing infrastructure. The user's data is outsourced and the user node receives control of the data, which has the same security risks as cloud computing. First off, it is challenging to guarantee data integrity because lost or incorrectly updated data from outsourcing could occur. Second, unauthorised parties might utilise the uploaded data for their own purposes. In the context of cloud computing, an auditable data storage service has been suggested to counter these dangers and safeguard data. In order to offer integrity, secrecy, and verifiability for a cloud storage system that enables a client to examine its data stored on untrusted servers, techniques like homomorphic encryption and searchable encryption are coupled.

II. LITERATURE SURVEY

[1] M A Manazir Ahsan et al.,

They put forth a system that hides data using the novel approach of XOR-Combination. Additionally, Block management outsources the results of the XOR combination to thwart malicious re-entry and to provide improved data recovery in the event of a loss. In addition, we provide a technique based on the hash method to make alteration detection easier and more likely.

[2] Rachna Arora et al.,

According to the article, using the internet to access a collection of computing resources that are owned and maintained by a third party is known as cloud computing. It is a method of distributing computing resources based on long-established technologies like server virtualization and is not a new technology.

[3] Raghul et al.,

Virtualization is suggested as the key phrase for such enabling technology for cloud computing. Physical computer equipment can be systematically divided using the virtualization technique into one or more virtual peripherals, each of which can be used and controlled to carry out computing operations. The user can break down these issues into services that can be integrated to deliver a solution with the use of cloud computing, which has adopted the SOA description.

[4] Zhihua Xia

Introduces a method that enables CPIR over the encrypted photos without giving the cloud server access to sensitive data. The feature vectors, which are accurate representations of the related images, come first. Then, to improve search efficiency, the pre-filter tables are built using locality-sensitive hashing. Next, the secure K-nearest neighbour (KNN) technique protects the feature vector.

[5] Cheng Guo et al.,

Give an example of a multi-phrase ranked search over encrypted cloud data that allows dynamic updating actions like adding or removing files. To keep track of the placements of keywords and determine whether a phrase appeared, we employed an inverted index. In order to rank the results and safeguard the privacy of the relevance score, this index can efficiently search for keywords.

III EXISTING SYSTEM

3.1 Overview

In conventional cloud computing, customers can no longer physically protect their data after outsourcing it to the cloud. A cloud service provider (CSP) can access, browse, or edit the data that is stored there. Additionally, due to a few technological issues, the CSP could unintentionally lose some data. Alternately, a hacker might compromise the user data's privacy. Confidentiality or integrity can be protected using some cryptographic processes (such as encryption, and hash chains). However, internal attacks cannot be stopped by cryptography methods.

3.2 Limitations

- Cloud computing has high latency when compared to fog computing.
- It does not provide any reduction in data while sending or transforming data.
- Cloud computing has less security compared to fog.
- Mobility is limited and has few number of server.

IV PROPOSED SYSTEM

4.1 Overview

We suggest a fog-based cloud storage system for data security, integrity, and availability in order to protect data. We suggest a technique known as Xor-combination that divides the data into various blocks, combines several blocks using the Xor operation, and outsources the resulting blocks to separate cloud/fog servers in order to ensure secrecy and availability (even after destructive occurrences). In our project, we successfully accomplish two objectives: data privacy and data recovery in the event of data loss. We increase the security of both cloud and fog servers.

4.2 Advantages

- Fog computing has low latency compared to cloud computing.
- It reduces the amount of data sent to cloud computing.
- Fog computing has high security than cloud computing.
- Mobility is a supporter and has a large number of server nodes.

4.3 System Design

A system architecture, sometimes known as a systems architecture, is the computational design that establishes a system's behaviour and/or organisational structure. A system's structural qualities are logically supported by an architecture description, which is a formal description of the system. It provides a roadmap from which items can be acquired and systems produced that will cooperate to accomplish the overall system, as well as a definition of the system components or building blocks.

4.4 System Testing

A crucial phase of every system development life cycle is system testing. The process of testing involves running software with the goal of identifying errors. It is impossible to overstate the value of software testing and its implications for software quality. Software testing serves as the final assessment of the specification, design, and coding and is a crucial component of software quality assurance. An excellent test case is one that has a decent chance of spotting an error that hasn't been found yet. Testing is done to look for mistakes. Testing is the process of looking for any flaws or weaknesses in a piece of work. It offers a means of examining the operation of parts, subassemblies, assemblies, and/or a finished product. It is the process of testing software to make sure that it satisfies user expectations and meets requirements without failing in an unacceptable way. Different test types exist. Every test type responds to a certain testing requirement.

A collection of tasks that can be planned ahead of time and carried out methodically is testing. The various test circumstances should be carefully examined, and any faults found should be addressed. To demonstrate that the software is error-free, the user's testing methodologies are put to use. Testing the system's dependability, completeness, and maintainability can be done in a variety of methods to achieve this.

V. SYSTEM IMPLEMENTATION

The proposed method's implementation stage is when the theoretical concept is transformed into a functional system. As a result, it can be said to be the stage that will determine whether a new system is a success and whether its users have faith in its ability to function well. Careful planning, research into the current system and its implementation limitations, creation of techniques to effect changeover, and evaluation of changeover methods are all part of the implementation stage.

5.1 Modules

5.1.1 User Process

a) New user registration

As a new user, user have to register themselves to upload and retrieve their files from the cloud. Once the user has registered then they can login using their user name and password.

b) View profile After registration user profile will be created. User can view and edit their profile if they need.

c) Upload file

When a user wants to upload their file into the cloud then the uploaded file option will come into the picture. When a user uploads their file one unique file key will be generated.

d) View uploaded file details

Once user uploaded their files then they can view their uploaded files in the view upload file tab.

5.1.2 Cloud process

a) Cloud login

In the cloud, user can login using their login credentials and view their profile details. They can also view their uploaded file details in the cloud.

5.1.3 Fog process

a) Lothe gin

In the fog server, user can login using their login credentials. They can view the user details. If they uploaded any files then that will be visible in the view uploaded file details section.

b) Block management

Block management is the process of dividing user files into three equal blocks, Which will be seen in the block management section users can also view that in view block management details section.

c) User file request

If the user wants to retrieve their files then they have to send a request, with the use of a file key generated when uploading the file. Then the fog server views the user request, verifies, and sends the files if an authorized user is requesting the file.

d) File download

Once the fog server verification process is completed, then the user can download their files in the file download section.

VI. PERFORMANCE METHODOLOGY AND RESULT

The data protection mechanisms in place, like encryption, have not been successful in thwarting attempts at data theft. We suggest a fog-based cloud storage system for data confidentiality, integrity, and availability in the proposed, the data are safeguarded confidentially, and integrity.

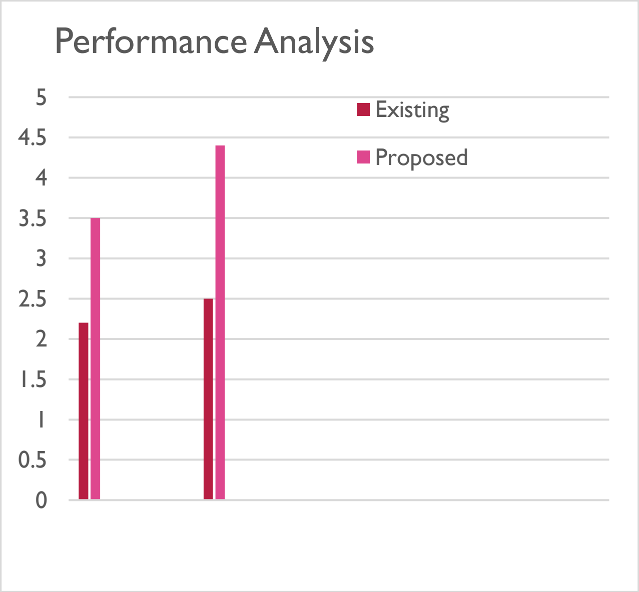

Figure 1: Performance analysis graph

Due to a lack of robust cryptographic methods, the system security in the current system is quite low. Because critical data is outsourced to the cloud, where it can be attacked from the inside or the outside, the suggested approach is safer.Due to several technical issues, the CSP may unintentionally lose data in the current system. In the suggested system, we employ a technique called XOR Combination to divide the data into many blocks. Utilize the XOR technique to combine numerous blocks, then distribute the resulting blocks to various cloud/fog servers.

VII. CONCLUSION AND FUTURE ENHANCEMENT

A secure solution for reliable cloud storage that is resistant to cyber threats should be based on a three-layer fog architecture. In this work, we put forth a plan that sends actual data in a twisted format to numerous cloud servers while carrying out preventive measures to a reliable fog server. We increased the effectiveness of the cloud storage service based on fog. In order to create a solid fog-centric cloud computing infrastructure, we strengthen the security of the fog server. It is feasible to further improve the efficacy of fog-based cloud storage services. A strong fog-centric cloud computing architecture can be built with better fog server security. It can be used to compute data that is secretive without revealing any of its contents.

REFERENCES

1. 1. B.Martini and K.-K. R. Choo (2014), "Distributed file system forensics: XtreemFS as a case study," Digital Investigation, vol. 11, no. 4, pp. 295-313.
2. C. Hooper, B. Martini, and K.-K. R. Choo (2013), "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, no. 2, pp. 152-163.
3. D. J. Fernández-Bretón (2018),"Hindman’s Theorem is only a countable phenomenon," Order, vol. 35, no. 1, pp. 83-91.
4. D. Quick and K.-K. R. Choo (2018), "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix," Future Generation Computer Systems, vol. 78, pp. 558-567.
5. J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato(2014), "Joint virtual machine and bandwidth allocation in a software-defined network (SDN) and cloud computing environments," in Communications (ICC), 2014 IEEE International Conference on, pp. 2969-2974: IEEE.
6. J. Feng, L. T. Yang, G. Dai, W. Wang, and D. J. I. T. o. B. D. Zou(2018), "A Secure Higher-Order LanczosBased Orthogonal Tensor SVD for Big Data Reduction".
7. J. Ni, K. Zhang, Y. Yu, X. Lin, X. S. J. I. T. o. D. Shen, and S. Computing(2018), "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing,".
8. J.Shen, D. Liu, J. Shen, Q. Liu, and X. Sun(2017), "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive and Mobile Computing, vol. 41, pp. 219-230.
9. J. Wang, T. Zhang, N. Sebe, and H. T. Shen(2018), "A survey on learning to hash," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 40, no. 4, pp. 769-790.
10. X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos(2017), "Knowledge-aware proactive nodes selection approach for energy management in the Internet of Things," Future generation computer systems.
11. Xiao Liu, Shanna zhao, N.Xiong (2019),”knowledge-aware proactive nodes selection approach for energy management in the internet of things”.
12. YuniLiu, Anfeng LShuanguang Guo, Zhetao Li, Young junechoi, H.Sekiya(2020)”context-aware collect data wenergynery efficiency in cyber-physical cloud systems”.
13. Y. Yang, X. Liu and R. Deng(2017), "Multi-user MultiKeyword Rank Search over Encrypted Data in Arbitrary Language," IEEE Transactions on Dependable and Secure Computing.
14. Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya (2017), "Context-aware collect data with energy efficient in Cyber-physical cloud systems," Future Generation Computer Systems.
15. Z. Xia, N. Xiong, A.V.Vasilakos, and X.Sun(2017), "EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," Information Sciences, vol. 387, pp. 195-204.
16. 16.Vithya Ganesan, B. Rahul, V. AnjanaDevi, Sri animaPadmini Viriyala, Ramya Govindaraj, Subrata Chowdhury, Jerry Chun-Wei Lin, “Block-chain based Smart Supply Chain and Transportation for Agri 4.0”, pages 135-156, Science Direct, April 2024.
17. Viswanathan Ramaswamy. Saikat Maity, N. Mohana Priya, Vithya Ganesan, Sri Anima Padmini, Subrata Chowdhury, Saurabh Adhikari, “Studies on Potential Conflicts of Network Densification in 6G”, pp 231-241, Proceedings of Second International Conference on Intelligent System, Springer Link, April 2024
18. Kennedy C Onyelowe, J Jagan, Denise-Penelope N Kontoni, Arif Ali Baig Moghal, Ifeanyichukwu C Onuoha,

R Viswanathan, Deepak Kumar Soni, Utilization of GEP and ANN for predicting the net-zero compressive strength of fly ash concrete toward carbon neutrality infrastructure regime, International Journal of Low-Carbon Technologies, Volume 18, 2023, Pages 902–914

19. Vithya Ganesan, k Vijaya Kumar, V Anjana Devi, P Ramadoss, “Hybrid Intelligence for Multimedia Data in Intra IoT (IIoT) Cloud by Persistent homology”, DOI: 10.1109/ACCAI53970.2022.9752558, International conference on Advances in computing, Communication and Applied Informatics (ACCAI), January 2022.