IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11740

PRIVACY PRESERVING CLOUD STORAGE WITH FOG COMPUTING

Niveditha S[1], Divakar H R [2]

Research Scholar, Dept. of MCA, P.E.S College of Engineering, Mandya, India[1].

Associate Professor, Dept. of MCA, P.E.S College of Engineering, Mandya, India[2].

Abstract: The fog nodes based cloud storage system is utilised to the confidentiality of information, validity, and the availability of information. We present the xor combination approach, which split the data document into numerous blocks, combines them by considering the xor operations, distributes those resulting block to various alternatives servers, for privacy and scalability. The suggested block management technique chooses the cloud storage to host each specified block of data, preventing any one cloud server from accessing a piece of the original data.

Keywords: Cloud computing, Fog Computing, Xor-Combination, Collision Resolving Hashing.

I. INTRODUCTION

Fog nodes is a private distributed network infrastructure known as fog computing which places data, compute, storage, and applications here between data devices and cloud. The advantages and strength of a cloud are made more accessible to the places where information is generated and used. Although it may also be done for compliance and security concerns, this is frequently done to increase efficiency. A fog nodes based cloud storage system is utilised to the confidentiality of information, validity, and the availability of information. We present the xor combination approach, which split the data document into numerous blocks, combines them by considering the xor operation, distributes those resulting block to various alternatives servers, for privacy and scalability. The suggested block management technique chooses the cloud storage to host each specified block of data, preventing any one cloud server from accessing a piece of the original data. Data preservation and retrieval from numerous sources are made possible by the Xor combination and blocks management, even when some blocks are missing. The collision resolving hashing and hashing mechanism, which are based on conventional hashes algorithms and can tolerate collisions, is also proposed in this project. When user information is sent to a fog node, which carries the same potential risks as cloud technology, the client loses control over the data and it is outsourced. The information that was outsourced could disappear or be mistakenly changed. The uploaded data may be used unlawfully by third parties for other purposes. An independently verifiable data storage service has been suggested in the cloud environments to safeguard the data from these dangers. Technologies like encryption algorithm and searchable encryption are paired in a cloud storage system to provide integrity, secrecy, and verifiability. This makes it possible for users to confirm their information on unreliable servers.

II. RELATED WORK

Alice Nineta R J et.al.,[1] prescribes a method that contains a strategy for sending real information in twisting form to several cloud storage while executing protective procedures on a dependable fog server. This paper approaches the work include CRH, Block Management, searchable encryption, and homomorphic encryption. By dividing and merging a dataset into fixed length blocks, homomorphic encryption gets a dataset ready for secure outsourcing. blocks management determines which combines the blocks should delivered to which cloud platform, limiting any one cloud from accessing all of the data or only a portion of it. To sum up, CRH supports effective identification of any modification. Security prediction shows that is computationally difficult to retrieve clear texts from such merged blocks. Similar to this, it identifies practically any malicious detection with a high probability and overcomes any hash function collision that may exist.

K.Maheshbabu et.al.,[2] proposes a cloud system that include the Cloud storage security concerns could prevent it from being widely used. Emerging cyber concerns against cloud storage include data loss, malicious modification, and privacy invasion. The main methods employed are the hash solomon codes and that is the custom hash algorithms, xorcombination and block managements to attain the goal. In order to safeguard data against illegal access, alteration, and destruction, this study proposes a safe cloud storage architecture that is fog-centric. Experimental findings support the suggested scheme's superior performance in terms of information processing speed when compared to contemporary alternatives.

DOI: 10.17148/IJARCCE.2022.11740

A.Kowsalya et.al, [3] proposes a system that includes some conditions includes symmetric algorithms were deployed on the cloud to test the effectiveness of numerous well-known cryptographic methods, including Identity-based cryptography and Proxy public key cryptography. This project suggests a safe cloud storage method focused on fog to guard against unauthorised data alteration and deletion. The proposal uses a new data concealment method called Or-Combination to prevent unauthorized. Additionally, Block-Management outsources Or-Combination outcomes to ensure greater recoverability in the event of data loss and to prevent malicious retrieval. Through security analysis, it also demonstrates the proposed scheme's robustness.

Sk. Asiff et.al,[4] proposes a system which proposes a fog computing-based secure cloud storage system that uses CRH operation, block management, and xorcombination. Blocks managements and the xorcombination are help to preserve privacy and stop data loss. The CRH Operation makes sure that data change is detected. Theoretical security study validates the confidentiality maintenance data recover, and modification of the proposed approach. Experiments on the systems were done in order to optimize the results of the experimental scheme to the current method. Results indicate that it is efficient in terms of time utilisation and memory.

BATTU NAVYA et.al.,[5] proposes a paper which provide a best feature to store and view the information from the clouds in a secure manner by utilizing the storage space and without wasting the storage space. The power of two concept, which fosters effective, fair collaboration and raises system utilisation overall, is the foundation of the proposed distributed protocol. In order to propose a decentralized system for fully cooperative fog computing, this is the initial stage.

Manazir Ahsan et.al.,[6] proposes a paper which includes safe fog computing-based cloud data storage system. In order to maintain confidentiality, this work uses Hash-Solomon code as well as the custom hash algorithms xorcombination, blocks managements, collisions resisting hashing. this paper proposes a technique based on hash algorithms to ensure the modifications detect of a highest probability and demonstrates robust the proposes scheme’s through privacy analysis. Final result confirms the suggested scheme’s increased performance compared to modern alternatives based on the duration of data processing.

III. METHODOLOGY

A. Fog Computing

Fog computing is a tiny version of a cloud computing which are in between the cloud servers and the client. This represents scenarios of fog node cloud storages system. The usr wants the reliable storage to save information, the user consists a full control on a fog device. Systems for fog computing can be used by users to manage their data. For advanced and powerful storage needs, fogcomputing device further communicates with several cloud. Additionally, a long, wide channel between the cloud and the fog and a short, thin channel between the fog nodes and the user help to overcome the communication problem (that is. transmission late). Information is uploaded by the client to the fog devices, which then use the mechanisms in the suggested schemes to divide the information into separate block and sends the various block to various cloud server. Multiple data blocks can be stored on a fog server's internal storage system. When the user requests data from the fog servers, the fog servers retrieves the necessary cloud servers blocks, combines them to create the needed information, and then sends it backs to the user. It makes use of many strategies for data loss detection and privacy preservation.

B. Xor Combination

A noble accepted for both data loss recoverability and privacy preservation is called Xor-Combination. This take in the padded information as inputs and outputs two set of tuples, and every of which is made up of a block tag and blocks of a predetermined length. There are numerous tuples in each collection. Splits padded input into a specified number of data blocks, each with a size, upon receipt. In reality, xorcombination is a set of instructions this is divides and joins any number of succeeding blocks in order to preserve security and enable data recovery in the event of a loss.

C. Collision Resolving Hashing

Collision resolving hashing is a technique based on a standard hashing algorithm that successful to check consistency even if there exists a collisions. The hash digest of original text is preserved in order to detect any malicious modification and Modified text has the same hash digest as that of original text. CRH is able to distinguish between original text and Modified text, despite having such collision. To improve the probability of detection, one can increase the number of random numbers and random digest pairs. However, given the property of standard collision resistant hash function, we prefer to conduct with one pair of random numbers and random digest in our scheme.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11740

D. System Architecture:

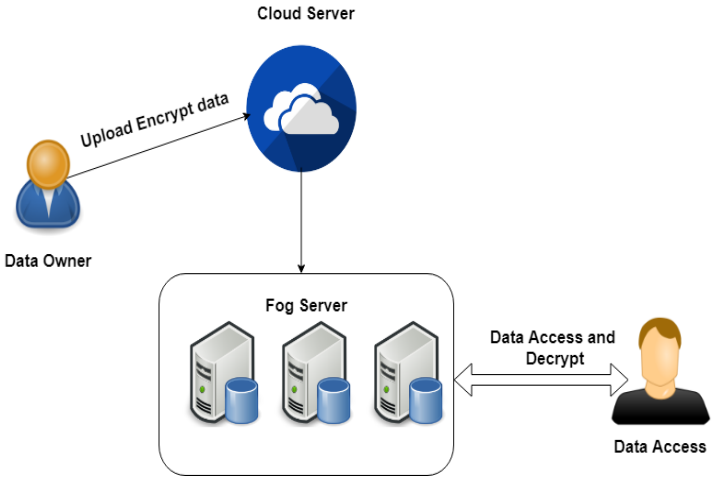

Fig 5.2 architecture diagram

In this model known as the systems architecture outline systems structurse, behavior, and the other aspects. An architectures description are formal descriptions and representation of system set up to facilitate analysis of its components structures and actions.

The system architecture shows the brief working of the system. The owners upload their data to the cloud in document format. The document stored in the cloud is hacked by unauthorized user. In order to secure the information we propose a three layer architecture that contains cloud layer, fog layer and edge layer. The document uploaded by the owner will stored to the cloud and that will send to the different fog nodes. In a fog server the data is split into number of fog nodes according to the document size. By implementing the hash algorithm to generates different hash codes to the different fog nodes. In the full efficiency model the hash code will change even one bit of data changes in the data. The data stored in a encrypted format to the fog nodes. The users try to view the data stored in a different fog node it resulted to show the encrypted data. Then the user is requested the admin to view the decrypted file. The admin sent the secret key to the user through the user email and the secret key will be unique for every user requests. The user login and view the decrypted data by entering a secret key sent by the admin and download the file.

D. Flowchart of implementation

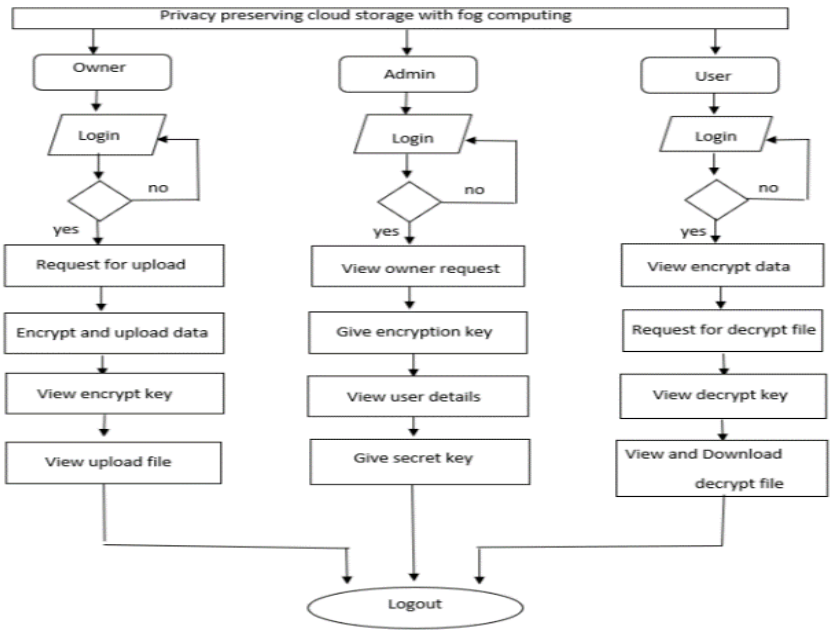

Fig: flow of implementation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11740

The Data Owner shall upload files in File Upload page. The file number will be automatically generated. So, the Data Owner need to specify only file name. Owner needs to upload the file by selecting choose file option. The uploaded file name will be displayed after selecting the file. Data Owner can click on upload button. The file uploaded by the Data Owner is split into 3-4 parts namely fog server 1, fog server 2 and so on according to the size of the file. The file is split into few parts to ensure security of data or content in the file. The Data User after login can search the required file with the file name. A list containing similar file names will be displayed. The Data User shall be able to go through the file request details. This is possible with the help of view file requests tab. The file contains details like User id, Username, Email id, File name, Status of file request and action button to view further details. The request is verified by admin then the secret key is shared to register mail by using the key user can view decrypted file details and can download it.

IV. IMPLEMENTATION

The Data Owner can login through this page by using registered username and password. New Data Owner must register with basic details in the link "New Owner Register Here" provided below login option.
New Data Owner must register with basic details. Data Owner must provide Name, Email id, Username and Password. Password should be entered twice to ensure confirmation of the given password. After providing the specified details the data owner needs to click register button and then will get a popup message as registered successfully. The Data Owner shall upload files in File Upload page. The file number will be automatically generated. So, the Data Owner need to specify only file name. He needs to upload the file by selecting choose file option. The uploaded file name will be displayed after selecting the file. Now Data Owner can click on upload button. The file uploaded by the Data Owner is split into 3-4 parts namely fog server 1, fog server 2 and so on according to the size of the files. This file is splits into few part to ensure security data or content in the file. After the Data Owner uploads the file a popup message "File uploaded successfully" will be displayed to ensure confirmation that the file has been uploaded successfully. Data User can login through this page by using registered username and password. New Data User must register with basic details in the link "New User Register Here" provided below login option. The Data User after login can search the required file with the file name. A list containing similar file names will be displayed. The Data User can send request to get the file which is required. The send request button will be given with the file name in the list. The admin will receive the request. A popup message "request sent successfully" will be displayed after Data User sends the file request.The Data User shall be able to go through the file request details. This is possible with the help of view file requests tab. The file contains details like Userid, Username, Email id, File name, Status of file request and action button to view further details. Admin can login through this page by using registered username and password through this portal. After Admin login to the portal, Admin can view the file requests sent by various Data Users. The list contains the details like Userid, Username, Email id, Filename, status and action tab. It contains details of the Data Users. Admin can accept the request sent by Data Users after verifying the required details. A key which is confidential shall be remitted to the Email id of the Data User as soon as Admin accepts the request sent by the such Data User. The Data User can login after receiving secret key by mail. The key is confidential. The user needs to submit the key in the file request view page by clicking on "View" button given beside the respective file name. A box appears displaying to enter secret key after clicking view button. The Data User shall now be allowed to view the requested data file and also download it after entering the correct secret key sent by the Admin.

V. RESULT AND ANALYSIS

In Proposed system, we implement fog-based cloud storage scheme for data confidentiality, integrity and availability. For confidentiality and availability, this project proposes a method referred to as Xor Combination that splits the data into several blocks, combine multiple blocks using Xor operation and outsource the resulted blocks to different cloud/fog servers. Xor indicates dataset by dividing and combineding into fixed length block's. Block Management decide to combined block's to be outsourced and cloud can retrieve the original data or a piece of data. By implementing the hash algorithm to generates different hash codes to the different fog nodes. In the full efficiency model the hash code will change even one bit of data changes in the data. The proposed system provide security to the document uploaded by the user. Without authentication by the admin user cannot access the file in the fog node.

VI. CONCLUSION

A system that could only successfully recognise static signs and alphabets has grown to be able to understand dynamic motions that happen in nonstop streams of images. The development of a complete lexicon for sign language recognition systems is currently the main focus of research. A number of academics are developing their own sign language recognition systems using their own databases and a restricted vocabulary. A considerable database that was developed

DOI: 10.17148/IJARCCE.2022.11740

is currently inaccessible for some of the countries using sign language recognition devices. The neural network is one of the more effective methods for pattern recognition and identification systems.

REFERENCES

[1] Ms. Alice Nineta R.J, Ms. Lini Raj L.A, " A Fog-Centric Secure Cloud Storage Scheme," International Journal for Research Trends and Innovation, 2020 IJRTI | Volume 5, Issue 4 | ISSN: 2456-3315.
[2] K.Maheshbabu A.SRINIJA C.SINDHU.,"A FOG-CENTRIC SECURE CLOUD STORAGE SCHEME," Journal of engineering science,Vol 12,Issue 08, AUG /2021 ISSN NO:0377-9254.
[3] A.Kowsalya, K.PRAVEENA., " A FOG-CENTRIC SECURE CLOUD STORAGE SCHEME," International Journal of Science & Engineering Development Research, Volume 5 Issue 6, June-2020
[4] Mr. Sk. Asiff, et.al. "An Efficient and Privacy Preserving Cloud Storage
Scheme in Fog Computing" Mukt Shabd Journal Volume IX, Issue VII, JULY/2020 ISSN NO : 2347-315.
[5] K.Rambabu, et.al.,"TOWARDS FOG CENTRIC SECURE CLOUD STORAGE SCHEME" International Journal of Creative Research Thoughts (IJCRT) 2021 IJCRT | Volume 9, Issue 6 June 2021 | ISSN: 2320-2882
[6] S. Basu et al., "Cloud computing security challenges & solutions-A survey," in Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual, 2018, pp. 347-356: IEEE.
[7] T. Wang, J. Zhou, X. Chen, G. Wang, A. Liu, and Y. Liu, "A Three-Layer Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 3-12, 2018.
[8] H. J. Syed, A. Gani, R. W. Ahmad, M. K. Khan, and A. I. A. Ahmed, "Cloud Monitoring: A Review, Taxonomy, and Open Research Issues," Journal of Network and Computer Applications, 2017.
[9] T. Wang et al., "Data collection from WSNs to the cloud based on mobile Fog elements," Future Generation Computer Systems, 2017.
[10] Y. Liu, A. Liu, S. Guo, Z. Li, Y.-J. Choi, and H. Sekiya, "Context-aware collect data with energy efficient in Cyber–physical cloud systems," Future Generation Computer Systems, 2017.