INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

Fog assisted IoT Enabled Patient Health Monitoring in Smart Homes

KADALI NAGA VENKATA SAI SANDEEP	Mr. NAGA. SRINIVASA RAO*
PG Scholar, Department of M.C.A,	Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College, Amalapuram, E.G.Dt., A.P, India.	S.K.B.R P.G College, Amalapuram, E.G.Dt., A.P, India.
sandeepsai1436@gmail.com	naagaasrinu@gmail.com

Abstract—

Cloud computing is presently being utilized as a planned elective for catering capacity benefit. Security issues of cloud capacity are a potential obstruction in its broad selection. Security breach, pernicious alteration and information misfortune are rising cyber dangers against cloud capacity. As of late, a haze server based three-layer design has been displayed for secure capacity utilizing different clouds. The fundamental procedures utilized are Hash-Solomon code and customized hash calculation in arrange to achieve the objective. In any case, it come about in misfortune of littler parcel of information to cloud servers and fizzled to supply superior alteration discovery and information recoverability. Th is paper proposes a novel fog-centric secure cloud capacity conspire to ensure information against unauthorized get to, alteration, and devastation. To avoid ill-conceived get to, the proposed conspire utilizes a modern strategy Xor - Combination to conceal information. Additionally, Block - Management outsources the result of Xor – Combination to avoid pernicious recovery and to guarantee way better recoverability in case of information misfortune. At the same time, we propose a based on hash calculation in arrange to encourage adjustment .

Index Terms*:* Cloud storage, fog server, Xor-Combination, CRH, privacy.

I. Introduction

CLOUD computing, a well-known computing paradigm, was introduced in SES 2006 (Search Engine Strategies 2006) and formally defined by NIST (National Institute of Standards and Technology) [1] in 2009. Since then, this technology has led to an increasing market share with its powerful computing, storage and communication facilities [2, 3]. Its infrastructure resources are not only scalable on demand, but are also available at a low price with a convenient payment policy, pay-as-you-go. In addition to consumer and corporate customers, cloud computing is also attracting the attention of many research communities, which are making massive efforts to gradually mature it. Therefore, cloud computing has many functionalities and cloud storage technologies are becoming increasingly important for the growing volume of data. The volume of user data increases exponentially with increases in network bandwidth [4]. Almost every internet user has their own cloud storage, ranging from GB to TB. Local storage alone cannot meet these immense storage needs. Most importantly, people inherently have a need for ubiquitous access to their data. Consequently, people are finding new media to store their data. A growing number of users who prefer powerful storage capacities have switched to cloud storage. they even prefer to store their private data in the cloud. Storing data on commercial public cloud server will be a prevailing trend in the near future. Many organizations like Dropbox, Google Drive, iCloud and Baidu Cloud take inspiration from this and offer a variety of storage services to their users. However, the benefits of cloud storage come with a range of cyber threats [5-8]. Privacy issues are one of the biggest threats along with data loss, malicious modifications and server crashes. These are some examples of cyber threats. There are some prominent cyber incidents in history, for example, hackers disclosed three billion Yahoo accounts in 2013, Apple's iCloud leak in 2014, Dropbox privacy breach in 2016, notably the iClouds leak event, in which numerous private photos of Hollywood actresses were disclosed caused a massive outcry. Such incidents have a lasting negative impact on the company's reputation [9-11]. In traditional cloud computing scenarios, once offloaded to the cloud, users can no longer physically protect their data. Cloud Service Providers (CSP) can access, search or modify their data stored in cloud storage. At the same time, the CSP may lose the data unintentionally due to some technical errors. Alternatively, a hacker can violate the privacy of user data. Confidentiality or integrity can be protected with some cryptographic mechanisms (such as encryption, hash chain) [12]. However, the cryptographic approach cannot prevent internal attacks, no matter how much the algorithm improves.Privacy Preserving Cloud Storage Scheme Based on Computational Intelligence in Fog Computing [13].

II. Related Work

Importance of cloud storage draws attention of scientists from both academia and industry. Data collection from WSNs to the cloud based on mobile Fog elements [14]. Improving the performance of the cloud storage as well as maintaining the security level are the main research domains. Security issues are always the focus of research in order to enhance reliability of the storage mechanisms [15]. A range of survey papers indicated that privacy breaches, malicious change (or integrity violation), data loss are the main cyber threats of cloud storage. Kaufman argued that, to cope with the above-mentioned experienced security threats, cloud servers have to establish coherent and effectual policy. Zissis et al. evaluated cloud security by identifying unique security requirements and presented a conceptual solution using trusted third party (TTP). As underlying cryptographic tool they used public key cryptography to ensure confidentiality, integrity and authenticity of data and communication while addressing specific vulnerabilities. Wang et al. focused on integrity protection on cloud computing and proposed public auditability scheme as a counter measure. They set two aims of their work, one was the efficient public auditing without requiring local copy of data and the other one was not to cause any vulnerability of the data. They utilized homomorphic authenticator with random masking for privacy preserving public auditing of cloud data. However, public key centric homomorphic authenticator caused computational burden and this work did not concentrate on partial/entire data loss. An efficient public auditing protocol using sampling block-less verification was proposed. At the center of their proposed protocol there was a noble dynamic data structure which consisted of doubly linked info table and a location array. This structure reduces the computation/

communication cost substantially. Conversely, like previous scheme, it does not address cyber threats other than integrity checks. Xia et al. proposed a mechanism titled Content Based Image Retrieval (CBIR) to protect image outsourced to cloud server relying on locality sensitive hashing (LSH) and secure k-nearest-neighbors (KNN) algorithms. It is equally applicable to other data types (i.e., text) as well.

III. Fog Computing

A fog computing node can be any network device with storage, computing and networking capabilities (routers, switches, video surveillance cameras, servers, etc.). Security and privacy issues predominate in fog computing infrastructures. The security and privacy issues can be mitigated by the mentioned counter technologies like proper authentication, access control, secure channels, intrusion detection, trust management. While all these techniques are in place, fog computing can be considered a trusted device that users can rely on for processing, storing and managing data. This paper introduces fog computing as a trusted device. Based on fog computing, the present research proposes a secure cloud storage scheme.

IV. Proposed Scheme

In terms of cloud data protection, we proposed a secure cloud data storage scheme based on fog computing. The proposed scheme assumes that the fog server, equipped with some computing, storage and communication capabilities, is reliable for the user. Reliable fog computing can be implemented using appropriate authentication, access control, and intrusion detection mechanisms. The proximity of the fogger to the user increases its credibility as a secure computing infrastructure. Apart from the fog calculation, the proposed scheme uses its own techniques, and $Xor{-}Combination$, $Block{-}Management$ and CRH.

The fog device processes the steps as follows:

It pads the data if the data is not an (exact) multiple of a fixed-length (L) block. - After that, it performs an XOR combination on the padded data, resulting in a number of 2-block combinations and a number of n 3-block combinations. - Then decides which blocks should be kept in which clouds and sends the blocks to the corresponding clouds. Various metadata (i.e. data number, block tag, ID, cloud number).At the same time, the Fog server performs a CRH operation on each of the generated data blocks. It calculates hash digest of a specific data block, generates random number R, calculates hash digest of data concatenated with random number R (tag combination), , random number (R), in fog database;- Finally, fog server stores the different blocks to different cloud servers.

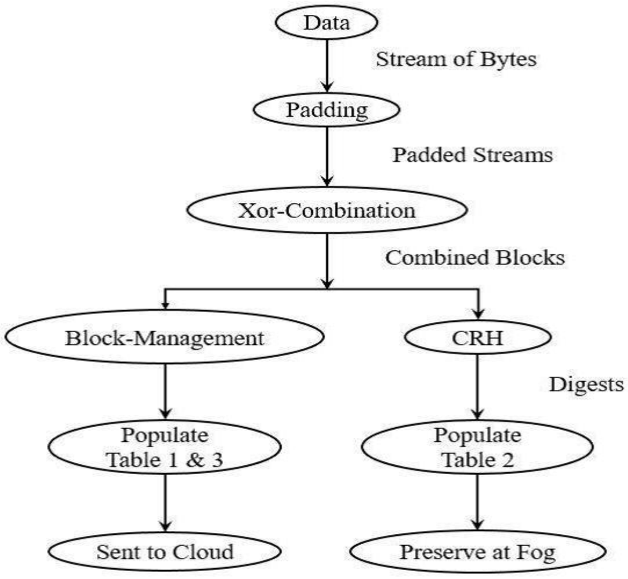


Fig. Data processing flow

Xor-Combination:

Xor-Combination is a noble approach used for privacy preservation and data loss recoverability simultaneously. It receives the padded data as an input and returns two sets of tuples as output where each tuple consists of a $blocktag$ and fixed length (L) blocks. Comma separated block number is termed as $blocktag$.

Block Management

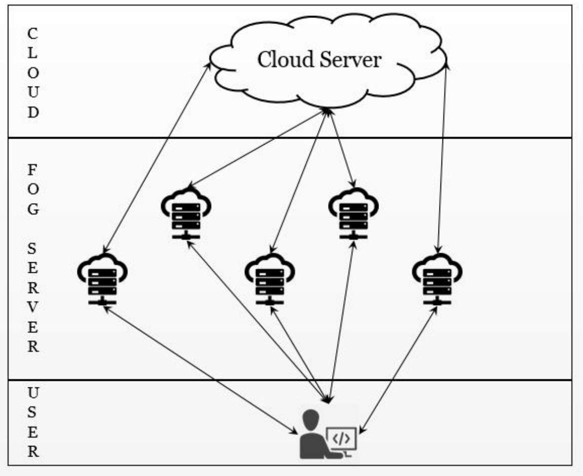
$Block - Management$ technique assists to figure out which blocks are to be stored in which cloud servers. It works on the combined blocks (i.e. 2-block-combinations and 3-block-combinations) generated from $Xor - Combination$. The block management along with $Xor–Combination$has two goals to attain, one is privacy of the data and the recoverability of the data in case of data loss

Collision Resisting Hashing (CRH):

$CollisionResistingHashing$ is a proposed technique based on a standard hashing algorithm (i.e. MD5, SHA256) that successfully checks consistency even if there exists a collision.

V. System Model

There are three entities in our system model: user, fog server, cloud server. The trust level of these entities is different. As with previous schemes, we consider the following entity reliability:



Fog based Server

User: The user is the owner of the data. Data protection, disaster recovery, user data change detection are the ultimate goal of this document.

FogServer: The Fog server is familiar to the user. The user relies on the Fog server for their data. The proximity of Fog devices to the user, robust physical security, proper authentication, secure communications, and intrusion detection ensure the reliability of Fog servers to the user.

Cloud Server: Cloud servers are considered honest but curious. This means that the cloud server is properly following the Service Level Agreement (SLA) but intends to analyse user data. Conversely, a cloud server can pretend to be good but act as a potential adversary. In this case, the cloud server can modify data to falsify it as original data. Similarly, the cloud server can hide/lose the data resulting in permanent data loss of the user. Additionally, hardware/software failure can result in data alteration or permanent loss.

VI. Storing and Retrieving Procedure

Storing Procedure:

Storing procedure takes a file to be securely uploaded to the cloud server. It has several steps and the most important steps take place on the Fog server. Fig. 4 shows the different steps and is described in the following section. When the user intends to upload a data file, he sends the file to the Fog server over a secure channel. Then the Fog server starts processing the file.

- **Splitting File:**The fog server fills the file as needed based on the system policy. After that, the Fog server splits the file into multiple blocks of fixed length and combines them withXor Combination algorithm.
- **Integrity Processing:** For each *combinedblock*, fog server generates random number, hash digest and random hash digest using CRH. Processing algorithm and stores this information into fog database for future integrity check.
- **Block Management*:*** fog server determines which block to be stored to which cloud server using *Block−Management* technique, stores this metadata into fog database and sends the blocks to respective cloud servers.
- **Cloud Storage*:*** Cloud server receives and stores the blocks along with metadata into its storage

Retrieval Procedure:

Retrieval procedure takes a request of a file, collects necessary *combinedblocks* from various cloud servers, and checks their integrity. If integrity check fails then it requests faulty blocks from other cloud servers. When all the necessary combined blocks pass integrity check, the fog server reconstructs the entire file and sends it back to the user.

- **Look up:**Once a user requests for a file to the fog server, the fog server looks up the relevant *combinedblocks* to construct the file into its metadata database. Afterwards it sends request to corresponding cloud servers holding the *combinedblocks*.
- **Integrity check*:***When the cloud servers send *combined blocks* back to the fog server, fog server checks integrity of each *combined block* using CRH. verification algorithm. If integrity check fails for a *combinedblock* then the fog server discards it and tries to reconstruct data block using other *combinedblock*s stored in other cloud server.
- **Reconstruction*:***Once the fog sever gets all the necessary combined blocks to derive the data blocks, it reconstructs the entire file. Finally, it sends the file back to the user.

VII. SECURITY ANALYSIS

- **Privacy Preservation**

The trusted Fog server processes the data, stores the metadata in its storage and uploads the data (hidden by the Xor combination algorithm) to the various cloud storages. Therefore, the cloud server only receives hidden data and without cooperation with the fog server, it cannot get the actual data. Also, the fog server uploads different pieces of data to different clouds. Therefore, even if a cloud server can retrieve the data, it only receives a fraction of the data. However, the proposed scheme does not want any information to go to the cloud server. Previous schemes [12, 13] using Reed-Solomon code or code derived from Reed-Solomon cannot hide small pieces of data from the cloud servers on which they are stored. On the contrary, we propose a noble technique to achieve the goals.

VIII. CONCLUSION

The advent of cloud computing has brought numerous benefits to the computing arena. The storage service is excellent unless users offload their sensitive data to a cloud storage server. The cloud server gets full access and control over user data as soon as data is offloaded to the cloud. It can read or browse the user data. In addition, data is vulnerable to many cyber attacks and malfunction of cloud hardware or software can permanently corrupt the data. Fog-based three-tier architecture matches secure cloud storage robust solution against cyber threats.

REFERENCES

1. Improving product marketing by predicting early reviewers on E-Commerce websites
S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Improving product marketing by predicting early reviewers on E-Commerce websites," Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. "Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN." Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40. Accessed 2 May 2024.

3. V. Srikanth, "CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS," IJTE, pp. 106–109, Jan. 2023, [Online]. Available: http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf

4. V. SRIKANTH, "DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS," International Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf

5. V. SRIKANTH, "A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES," IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023, [Online]. Available: http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Detection of fake currency using machine learning models," Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. "Cyberspace and the Law: Cyber Security." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. "Data Structures Laboratory Manual." IOK STORE,

www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

9. Data Analytics Using R Programming Lab." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)," journal-article, 2019. [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf

10. V. SRIKANTH, "Secured ranked keyword search over encrypted data on cloud," IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION," IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS," Feb. 2017. [Online]. Available: http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

14 Srikanth, V. 2018. "Secret Sharing Algorithm Implementation on Single to Multi Cloud." International Journal of Research 5 (01): 1036–41. https://journals.pen2print.org/index.php/ijr/article/view/11641/11021.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. "Intelligents Traffic Light Controller for Ambulance." Journal of Image Processing and Intelligent Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, https://doi.org/10.55529/jipirs.34.19.26. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. "Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges." Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023, pp. 1–7, https://doi.org/10.55529/jeet.35.1.7. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21,

https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023