International Journal of Science Engineering and Advance Technology (IJSEAT)
ISSN 2321-6905, Vol. 8, Issue 3, March -2020

A secure cloud storage scheme on fog computing- *Xor−Combination*, *Block−Management* and *CRH* operation

[1]A.Tejaswi Gurunath, [2]K.V.V.L.Madhuri
[1]Final year student, M.Sc(CS), Dept. of Computer Science, Ideal College of Arts & Sciences, Kakinada, AP,India
[2]Assistant professor, Dept. of Computer Science, Ideal College of Arts & Sciences, Kakinada, AP,India

ABSTRACT:
Fog server based three-layer design has been introduced for secure storage employing multiple clouds. The fundamental methods utilized are Hash-Solomon code and redid hash algorithm so as to achieve the objective. However, it brought about loss of littler part of data to cloud servers and neglected to give better change location and data recoverability. It proposes a novel haze driven secure cloud storage plan to ensure data against unapproved access, alteration, and obliteration. To forestall ill-conceived get to, the proposed plot utilizes another system *Xor−Combination* to cover data. Also, block management outsources the results of *Xor−Combination* to forestall pernicious recovery and to guarantee better recoverability if there should arise an occurrence of data misfortune. At the same time, we propose a procedure dependent on hash algorithm so as to encourage alteration detection with higher probability.

KEYWORDS: Cloud storage, fog server, Xor-Combination, CRH

1] INTRODUCTION:

Cloud computing is a general term for whatever includes conveying facilitated benefits over the Internet. These administrations are comprehensively isolated into three classifications: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was motivated by the cloud image that is regularly used to speak to the Internet in flowcharts and charts. A cloud administration has three particular qualities that separate it from protocolal web hosting. It is sold on request, commonly constantly or the hour; it is flexible - a client can have so a lot or as meager of a help as they need at some random time; and the administration is completely overseen by the supplier (the buyer needs only a PC and Internet get to) [1,5].

Revised Manuscript received on February 15th , 2020
*Corresponding Author
A. Tejaswi Gurunath
mail id- tejaswi1987@gmail.com

Huge advancements in virtualization and cloud computing, just as improved access to fast Internet, have quickened enthusiasm for cloud computing. A cloud can be private or public.An public cloud offers administrations to anybody on the Internet. (As of now, Amazon Web Services is the biggest open cloud supplier.) A private cloud is an exclusive system or a server farm that provisions facilitated administrations to a predetermined number of individuals. Private or public, the objective of cloud computing is to give simple, scalable access to processing assets and IT services.

2] LITERATURE SURVEY:

T. Wang, J. Zhou, X. Chen, We propose a three-layer storage system dependent on haze registering. The proposed system can both exploit cloud storage and secure the protection of data. Furthermore, Hash-Solomon code algorithm is intended to isolate data into various parts. At that point, we can place a little piece of data in neighborhood machine and haze server so as to secure the protection[6,8,13]. Besides, in light of computational insight, this algorithm can process the dispersion extent put away in cloud, haze, and neighborhood machine, individually. Through the theoretical safety analysis and test assessment, the possibility of our plan has been approved, which is actually an amazing enhancement to existing cloud storage scheme[9,10].**T .Wang [13,14]** We propose a productive open examining protocol with worldwide and testing blockless check just as cluster inspecting, where data elements are significantly more proficiently bolstered than is the situation with the cutting edge. Note that, the novel powerful structure in our protocol comprises of a doubly connected data table and an area exhibit. In addition, with such a structure, computational and correspondence overheads can be decreased significantly. Security examination demonstrates that our protocol can accomplish the ideal properties.

3] PROBLEM DEFINTION:

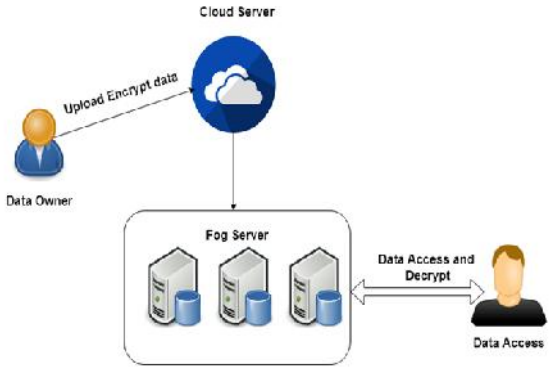
In cloud computing, when clients redistribute their data to the cloud, they can no longer secure it truly.

Cloud Service Provider (CSP) can access, look or adjust their data put away in the cloud storage. Simultaneously, the CSP may misfortune the data unexpectedly because of some specialized shortcomings. Alternatingly, a programmer can disregard the security of the client data. Utilizing some cryptographic instruments, (for example, encryption, hash chain), privacy or uprightness can be ensured.Notwithstanding, cryptographic methodology can't forestall interior assaults, regardless of how much the algorithm improves. To secure data secrecy, integrity and availability (CIA), a few research networks presented Fog Computing putting haze devices in the middle of the client and the cloud server.

4] PROPOSED APPROACH:

In Proposed framework, mist basedcloud storage conspire for data secrecy, respectability and accessibility. For privacy and accessibility, we propose a technique alluded to as Xor Combination that parts the data into a few blocks, join numerous blocks utilizing Xor activity and re-appropriate then came about blocks to various cloud/fog servers. So as to forestall any individual cloud server to recover a segment of unique data, the proposed system block administration chooses the cloud server to store every specific datablocks. Xor mix alongside block administration assists with shielding data and to recover data from different sources in any event, when a few blocks are absent. Simultaneously, we propose a respectable hashing system titled as Collision Resolving Hashing (CRH) activity dependent on protocolal hash algorithm that withstands impact in hashing and security highlights. The proposed plot flourishes to be a hearty answer for effective and secure cloud storage.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

6.1] Cloud Server

Cloud server is considered as legitimate yet inquisitive. This implies cloud server follows the Service Level Agreement (SLA) appropriately, yet has a goal to dissect client's data. Then again, cloud server may claim to be acceptable however goes about as a potential foe. All things considered, cloud server may adjust data so as to manufacture as unique data. So also, cloud server may stow hide/loss the data bringing about perpetual data loss of the client. Besides, hardware/software failuremay bring about data adjustment or permanent loss as well.

6.2] Fog Computing

Fog processing is littler form of cloud computing that is set between cloud server and the client. It shows the situation of mist basedcloud storage framework. As client needs a dependable stockpiling to spare data, the client has full command over haze devices. Clients can depend on haze computing/storage devices for the management of their data. Fog computing devices further communicate with multiple clouds for cutting edge storage requirements. Also, long-thick channel between cloud-haze and short-dainty channel between mist client adds to determine the correspondence issue (i.e. transmission delay). The user uploads the data to the fog devices, fog device utilizes the techniques of proposed scheme to split the data into different blocks and send the different blocks to different cloud servers. Fog server can store several blocks of data to its own storage system.

6.3] Privacy Preserving

Trusted fog server processes the data, stores the metadata into its storage and uploads the data to the different clouds' storages. Therefore, cloud server only gets hidden data and without collaboration with fog server, it cannot retrieve the actual data. Besides, fog server uploads different portions of data to different clouds. Thus

even if a cloud server is able to retrieve the data, it only gets a fraction of data.

6.4] 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 block tag and fixed length blocks. Each set contains number of tuples. Upon receiving padded input, splits it into numbers of data blocks with size.Xor Combination actually, is a series of code that splits and combines any number of

consecutive blocks to facilitate privacy preservation and recoverability in case of data loss[15].

6.5] Collision Resolving Hashing

Collision Resolving Hashing is a proposed technique based on a standard hashing algorithm that successfully checks consistency even if there exists a collision. 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 originaltext. CRH is able to distinguish between OriginaltextandModifiedtext, despite having such collision[11,12].

7] ALGORITHM:

Input: Data as block of bytes.

Step 1: It takes 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.

Step 2: Upon receiving padded input, splits it into $\lceil |data||L| \rceil$ numbers of data blocks with size L each such as $B1,B2,B3,\ldots \ldots \ldots,Bn$

Step 3: Afterwards, it generates 2-block-combinations ($\boldsymbol{Ci}$,) and 3-block-combinations ($\boldsymbol{Ci,j,k}$) with consecutive data blocks. Considering first data block comes after the last data block like round robin.

Step 4: Perform Xor operation for 2-block-combinations ($\boldsymbol{Ci}$,) and 3-block-combinations ($\boldsymbol{Ci,j,k}$)

Step 5: Finally, each block can be retrieved using five different interactions between combined blocks in 2/3-Xor-Combination.

$Bi=Ci,+1,i+2 \oplus Ci+1,i+2$

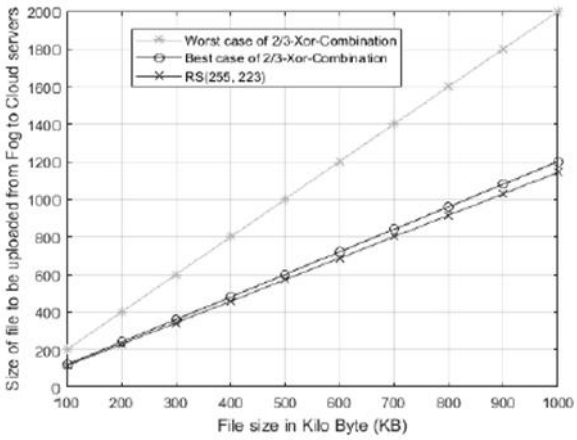
$Bi=Ci-1,,i+1 \oplus Ci-1,i \oplus Ci,i+1$

$Bi=Ci-2,-1,i \oplus Ci-2,i-1$

$Bi=Ci-3,-2,i-1 \oplus Ci-3,i-2 \oplus Ci-1,i$

$Bi=Ci+1,+2,i+3 \oplus Ci,i+1 \oplus Ci+2,i+3$

8] RESULTS:



Downloading time comparison using payload size.

9] CONCLUSION:

This paper presents Xor combination, CRH and block management approaches. Xor combination readies a dataset for outsourcing by parting and consolidating into fixed length blocks. Block Management chooses which consolidated blocks to be recloud to which cloud server with the goal that no individual cloud can recover the first data or a bit of data. Simultaneously, Xor combination, alongside Block the management, adds to remaking of any data block if there should be an occurrence of malicious modification or data loss.

10] EXTENSION WORK:

This domain can be summarized as follows: 1. To enhance the efficiency of fog based cloud storage service. 2. To improve the security of fog server for a robust fog centric cloud computing infrastructure. 3. To enable cloud server to compute cryptic data without revealing any data from it.

11] REFERENCES:

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Communications of the ACM, vol. 53, no. 6, p. 50, 2010.

[2] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in Internet of Things," Future generation computer systems, 2017.

[3] 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.

[4] 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 Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 2969-2974: IEEE.

[5] B. Martini and K.-K. R. Choo, "Cloud filesystem forensics: XtreemFS as a case study," Digital Investigation, vol. 11, no. 4, pp. 295-313, 2014.

[6] N. D. W. Cahyani, B. Martini, K. K. R. Choo, and A. Al-Azhar, "Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study," Concurrency and Computation: Practice and Experience, vol. 29, no. 14, 2017.

[7] J. Fu, Y. Liu, H.-C. Chao, B. Bhargava, and Z. J. I. T. o. I. I. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," 2018.

[8] C. F. Tassone, B. Martini, and K. K. R. Choo, "Visualizing digital forensic datasets: a proof of concept," Journal of forensic sciences, vol. 62, no. 5, pp. 1197-1204, 2017.

[9] C. Hooper, B. Martini, and K.-K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," Computer Law & Security Review, vol. 29, no. 2, pp. 152-163, 2013.

[10]D. Quick and K.-K. R. Choo, "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, 2018.

[11]Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study," Computers & Electrical Engineering, vol. 58, pp. 350-363, 2017.

[12]T. Wang et al., "Fog-based storage technology to fight with cyber threat," Future Generation Computer Systems, 2018.

[13]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.

[14]T. Wang et al., "Data collection from WSNs to the cloud based on mobile Fog elements," Future Generation Computer Systems, 2017.

[15]M.Xie, U. Bhanja, J. Shao, G. Zhang, and G. Wei, "LDSCD: A loss and DoS resistant secure code dissemination algorithm supporting multiple authorized tenants," Data Sciences, vol. 420, pp. 37-48, 2017.

Mr.A.TejaswiGurunath is a student of Ideal College of Art & Science, Kakinada Presently he is pursuing his M.Sc(Computer Science) from this college and he received his BSc from Government Arts College Rajahmundry affiliated to AdhikaviNannaya UniversityRajahmundry in the year 2018. His areas of interest includes Computer Networks andObject Oriented Programming languages, all current trends and techniques in Computer Science.

Ms.K.V.V.L.Madhuri is presently working as Assistant Professor in P.G Department of Computer Science, Ideal College of Arts& Sciences, Kakinada. She obtained her M.Sc in Computer Science from Andhra University. She has 2+ years of teaching experience at Post Graduate Level.Her areas of interest include Software Engineering, Data Structures, Database ManagementSystems, Computer Organization, Computer Networks.