International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

An Efficient Block Storage Mechanism for Cloud Computing Adoption Framework

K.V. Gowthami & K.Ganesh Reddy
M. Tech, Department of CSE, Shri Vishnu Engineering College for Women (A), Vishnupur, Bhimavaram, West Godavari District, Andhra Pradesh, India

Ph.D Associate Professor, Department of CSE, Shri Vishnu Engineering College for Women (A), Vishnupur, Bhimavaram, West Godavari District, Andhra Pradesh, India

Abstract— *Providing Data Security for huge amount of data in business cloud is important and difficult. Cloud Computing Adoption Framework (CCAF) is one of the frameworks which is used to provide the Security for business cloud. CCAF makes use of Business process Modelling Notation (BPMN) for Security measure. By using this BPMN, CCAF classifies into multi-layered Security. They are: - 1) Firewall 2) Identity Management and intrusion Prevention 3) Convergent Encryption. However, CCAF framework stores same data copy of multiple users is stored in multiple locations, instead of storing same copy information in one location. Due to this problem, cloud storage utilization is not effective. To overcome this problem, in our proposed effective storage approach, we have considered hash tables and id's of cloud user's at the cloud storage provider. Each client maintains its hash tables for storing and retrieving the data from storage cloud. Eventually, our proposed approach can identify the same data of multiple users or same user and it stores in one location, instead of storing multiple locations. Our results prove that block storage can effectively utilized in CCAF framework.*

Keywords: CCAF, FGSM, BPMN, Cloud Security, SHA1 Algorithm with Hash function

1. Introduction

Cloud computing is an advanced computing worldview which empower clients to get cloud benefits in anyplace at any spots. Presently days there are a few requests for the businesses to move their data in to the Cloud and bring together administration for server farms, administrations and applications and they are intended to accomplish fetched investment funds and operational efficiencies and security. In the meantime, arrangements and framework plan and sending in light of its present security practices ought to be guarantee all data and administrations are security consistent with up and coming patches.

A Security program need to build up a hazard based approach that perceives fitting controls will guarantee that all. The clients can be secured, and that data can be private, have respectability and be accessible to the clients constantly. The FIE and DE has been created to guarantee that all executions and administration conveyances can address all the specialized difficulties with a specific end goal to meet the prerequisites for Business Clouds. With the fast ascent in cloud computing, programming as an administration (SaaS) is especially sought after, since it offers benefits that suit clients' need. For instance, well being informatics can enable therapeutic scientists to analyze testing sicknesses and malignancies. Programming as an administration (SaaS) is especially popular with the fast ascent in cloud computing.

The server farms are confronting a few difficulties in expanding the data. Concentrate on the data security while encountering a substantial increment of data, if clients or customers collect many terabytes of data every day, regardless of whether they are from the outside sources or from the inner sources, for example, assault of infections or Trojans. This is an examination challenge for data security which is fundamental for the better administration of the server farm to deal with a fast increment in the data. Aside from the server farm security administration for quick development in data, the product building process ought to be sufficient strong to withstand the assaults and unapproved access to the client's data put away in the server farms. Budgetary investigation can guarantee precise and quick reproductions to be accessible for speculators. Training as an administration enhances the nature of instruction and conveyance. Portable applications enable clients to play web based recreations and simple to-utilize applications to cooperate with their associates.

While more individuals and associations utilize the cloud administrations, security and protection end up plainly vital to guarantee that every one of the data they

utilize and share are very much ensured. A few specialists declare that security ought to be executed before the utilization of any cloud benefits set up. This makes a testing adoption situation for associations since security ought to be authorized and executed in parallel with any administrations. Furtherly, the whole process should be possible with the advancement of framework to take care of the specialized plan and executions, administration and arrangements related with great practices to help associations accomplishing great Cloud outline, organization, movement and administrations. Despite the fact that associations that receive cloud computing recognize benefits offered by cloud administrations, difficulties, for example, security and protection remain an investigation for authoritative adoption. While supervising the significance of security, the product building and advancement process ought to dependably configuration, actualize and test security highlights.

This is an exploration challenge for data security which is basic for the better administration of the server farm to deal with a fast increment in the data. Aside from the server farm security administration for fast development in data, the product building process ought to be sufficiently hearty to withstand assaults and unapproved get to. The issue of Security and the dread of data robbery is on the ascent. There are even now and again when access to and control of data in the cloud winds up noticeably tricky. The issue could be that, innovations sent by specialist organizations for data assurance does not give a one-fit-all arrangement. The examination explores cloud security sending innovations and goes further to know whether there or not there exist strategy rules for CSPs in Ghana. One can't discard the way that, however there had been consistent rise of advances, there is additionally no auspicious security standard produced for developing innovations.

The whole process can be additionally solidified with the improvement of a framework to take care of the specialized outline and usage, administration and strategies related with great practices. This propels us to build up a framework, Cloud Computing Adoption Framework (CCAF), to help associations effectively embrace and convey any cloud administrations and ventures. In this paper, we exhibit our security plan, execution and answer for CCAF. At the end of the day, the present variant of CCAF needs correction by refreshing the security rules and business setting. A few security papers have stressed particularly on the hypothetical advancement and there is an absence of points of interest portraying how to duplicate comparative outcomes and repeat the accomplishment of conveying security administrations.

Second, security advancements, measures and arrangements ought to be effortlessly incorporated with the current practices. Third, the business setting will be accentuated, since the enhanced framework ought to be received by industry and businesses that go for long haul advantages, for example, cost diminishment, business openings, gainfulness, change in productivity and consumer loyalty. The improvement of security and business arrangements ought to be clear and simple to embrace.

A hash function takes a variable length message and creates a settled length message as its yield. This yield message is known as the hash or message process of the first info message. The trap behind building a decent, secured cryptographic hash work is to devise a decent pressure work in which each info bit influences however many yield bits as could be allowed. The SHA-1 algorithm has a place with an arrangement of cryptographic hash capacities like the MD group of hash capacities. Be that as it may, the fundamental contrast between the SHA-1 and the MD family is the more successive utilization of data bits over the span of the hash work in the SHA-1 algorithm than in MD4 or MD5. This reality brings about SHA-1 being more secured contrasted with MD4 or MD5 yet to the detriment of slower execution. The first determination of the algorithm was distributed in May 1993 though the amended rendition was distributed in 1995. The algorithm depended on standards like those in the plan of the MD4 and MD5 algorithms.

2. Existing System

Data assurance is top most security issue in cloud. Users data in the cloud are assaulted by programmers from outside Cloud Specialist organizations (CSP) called outcast assault and inside the CSP called insider assault. Assaults from inside the CSPs are exceptionally hard to be secured or to be distinguished. Users data sent to the cloud are controlled and observed by CSPs. CSPs as favored executives have the rights to investigate the client's data. In this way, there is a probability that insiders from CSPs assault the data. Users don't have any control of the data in cloud stockpiling. Also, cloud

is an open situation. Data may blend with other client's data. Users don't know whether the data is encoded in the cloud stockpiling or not. Keeping up keys for every client is more troublesome for CSPs, and a similar key is utilized for all user's data. Client's data must be in a settled configuration indicated by the specialist co-op, and henceforth the specialist co-op knows all the data required for understanding client's data. Here the data insurance issues are raised up.

3. Proposed System

Our proposed system is utilized for outlining and conveying the security arrangements. The approach is to utilize a structure that can incorporate distinctive parts of security. We propose the Fine Grained Security Show (FGSM), which offers the multilayered security layer for Cloud Registering administrations. Since each kind of security has its qualities and shortcomings, the mix of various security arrangements can improve the qualities and diminish the shortcoming if just a single arrangement is conveyed.

Before presenting the points of interest of our refreshed system, every component of the CCAF security is depicted or described as follows.

Identification is an essential and the principal procedure of setting up and recognizing among individual/client and administrator ids, a program/process/another PC ids, and data associations and interchanges.

Privacy is the way to keeping up the accomplishment of distributed computing and its effect on sharing data for long range interpersonal communication and cooperation on a particular undertaking. This can be kept up by enabling clients to pick when and what they wish to partake notwithstanding permitting encryption and decryption offices when they have to ensure particular data/ media content.

Integrity is characterized as a procedure of keeping up consistency of activities, correspondences, values, strategies, measures, standards, desires, and results. Moral esteems are vital for cloud specialist co-ops to secure integrity of cloud client's data with trustworthiness, honesty and precision at unequalled.

Durability is otherwise called, persistency of client activities and administrations being used ought to incorporate sessions and different sessions.

SHA1 Features:

• The SHA1 is utilized to figure a message process for a message or data record that is given as input.

• The message or data record ought to be thought to be a bit string.

• The length of the message is the number of bits in the message (the vacant message has length 0).

• If the number of bits in a message is varies of 8, for smallness we can speak to the message in hex.

• The motivation behind message cushioning is to make the aggregate length of a cushioned or original message varies of 512.

• The SHA1 consecutively forms blocks of 512 bits when registering the message p process.

• As a synopsis, a "1" trailed by m "0"s took after by a 64-bit integer are affixed to the finish of the message to create a cushioned message of length 512 * n.

• The 64-bit integer is l, the length of the first message.

• The cushioned or original message is then prepared by the SHA1 as n 512-bit blocks.

4. System Architecture

CCAF security software execution is exhibited by the utilization of the Fine-Grained Security Display (FGSM), which has layers of security instrument to permit multi-layered assurance. This can guarantee decrease in the diseases by Trojans, infection, worms, and spontaneous hacking and dissent of administration assaults. Each layer has its own particular assurance and is responsible for one or various obligations in the insurance, preventive estimation and isolate activity exhibited in Figure 1. Every one of the highlights in FGSM incorporate access control, intrusion detection system (IDS) and intrusion prevention system (IPS), this fine-grained security structure presented fine-grained border safeguard. The layer portrayal or description is as per the following.

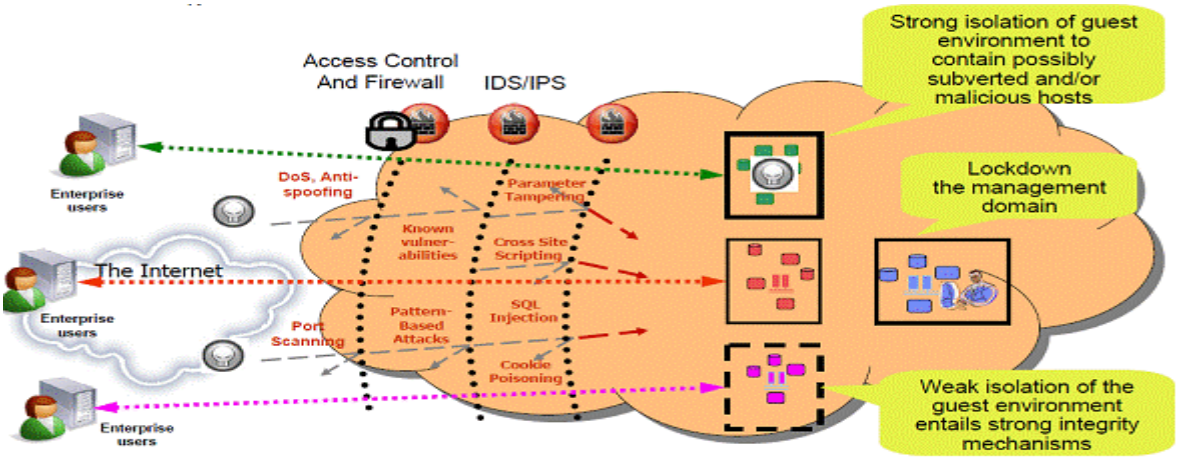

Figure 1: The Fine-Grained Security Model offered by CCAF

5. Block-level storage algorithm

1. User file is fragmented into ->(f1,f2,f3…..fn)
2. Create message digest for all fragments((f1,f2,f3…..fn))->H(M1), H(M2), H(M3)……,(Hn)
3. Use these H(M) values as key values K={k1,k2,k3……kn} to encrypt fragments $E_{ki}(f_i)$
4. Each $E_{ki}(f_i)$ is signed with User private key $(E_{ki}(f_i))_{Upub}$
5. Upon receiving $(E_{ki}(f_i))_{Upub}$ message by cloud owner
6. If $((E_{ki}(f_i))_{Upub}$ = Valid)
7. $E_{ki}(f_i)$ is encrypted with shared secret key Kws (cloud owner and storage servers) $(E_{ki}(f_i))$Kws
8. Else
9. $(E_{ki}(f_i))_{Upub}$ message is discarded
10. Storage server verifies the $(E_{ki}(f_i))$Kws with known shared key
11. If $((E_{ki}(f_i))$ Kws = Valid)
    $E_{ki}(f_i)$ is matched with any existing cloud storage $E_{ki}(f_i)$ indexed in already existed $E_{ki}(f_i)$ in the storage server along with the user id.
12. Else
13. $(E_{ki}(f_i))$ Kws message is discarded
14. User uses message digest H(M) to get the file from storage server

Algorithm Description:

- Normal file is divided into sub files like file1, file 2.file 3, file 4, file 5… file n.
- Create a Message Digest Algorithm (MD5) for splitting up all the files and apply Hash function to the files.
- Use this Hash function of the file as Key values where it is used to encrypt the files as the encrypted fragments.
- Here, each encrypted fragment is assigned to a User Private Key.
- The Cloud owner is responsible of receiving the encrypted fragment files.
- If the encrypted fragment file message is valid then it will share the private key to the cloud owner and store under the Storage Server.
- Else the message file will be discarded.
- The Storage Server verifies whether the encrypted file message is valid or not with the known shared key.
- So that if encrypted key is matched with the existing cloud storage, then it will be stored in the storage server along with the user id.

- Otherwise, the key message will be discarded.
- Finally, User must use the Message Digest H (M) by using SHA Algorithm to get the file from the Storage Server.
- Here, This Algorithm describes about how the File is fragmented and applies the algorithm and Hash functions to the files and will assign the private keys in an encrypted manner. Finally checks whether it is valid or not. If valid it will store in Storage Server or otherwise the message will get discarded. And uses Message Digest to find the file from the Storage Server.
- Actually, a secure hash algorithm is actually a set of algorithms developed by the National Institutes of Standards and Technology (NIST) and other government and private parties. These secure encryption or "file check" functions have arisen to meet some of the top cyber security challenges of the 21st century, as a number of public service group's work with federal government agencies to provide better online security standards for organizations and the public.
- In cryptography, **SHA** (Secure Hash **Algorithm**) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long.
- All of these secure hash algorithms are part of new encryption standards to keep sensitive data safe and prevent different types of attacks.

6. Results

Table 6.1: User data storage1

Contents	Values
Existing system	8136.40
Proposed system	3550
Without any mechanism	9600

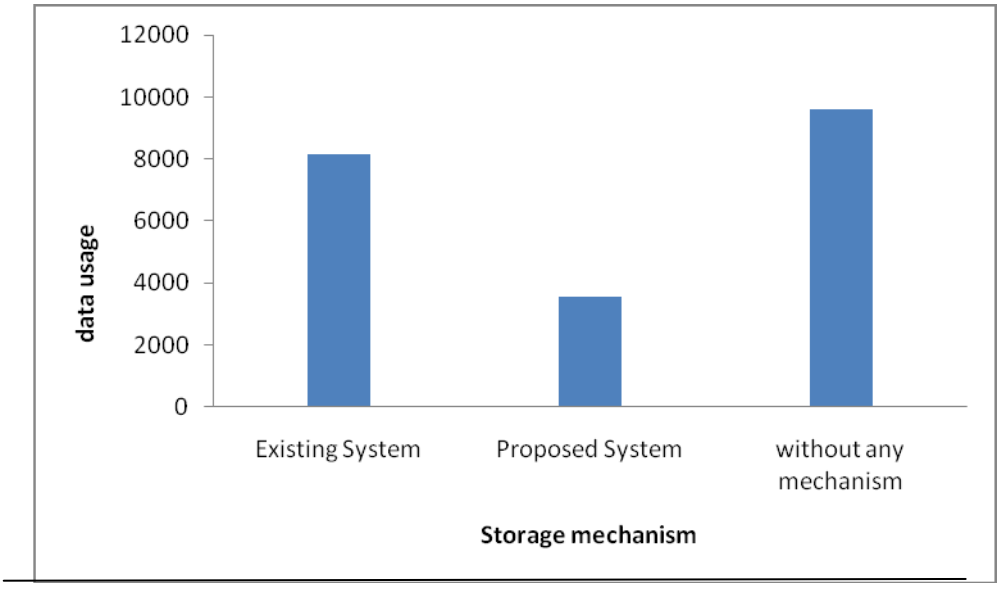

Fig 6.1 : User Data Storage1 Graph

In existing system, we got value like 8136.40. Whereas, in proposed system we got values like 3550. But we got value like 9600 without any mechanism.

Table 6.2: User Data Storage2

Contents	Values
Existing	2131.28
Proposed	1600
Without any mechanism	2400

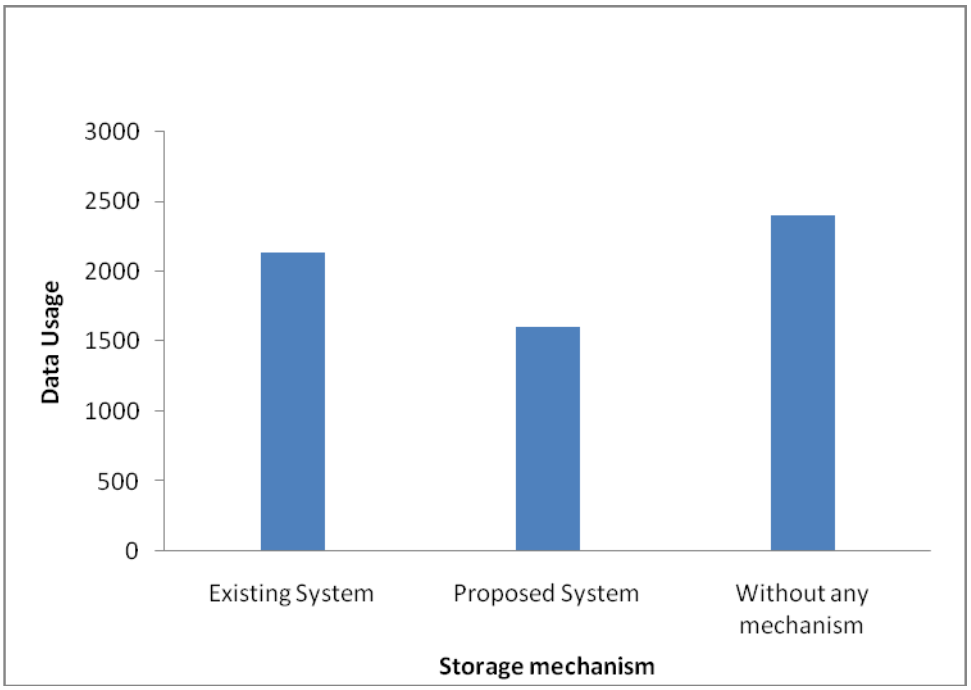

Fig 6.2 : User Data Storage2 Graph

In existing system, we got value like 2131.28. Whereas, in proposed system we got values like 1600. But we got value like 2400 without any mechanism.

Table: 6.3 User Data Storage3

Contents	Values
Existing system	1599.17
Proposed System	1300
Without any mechanism	1800

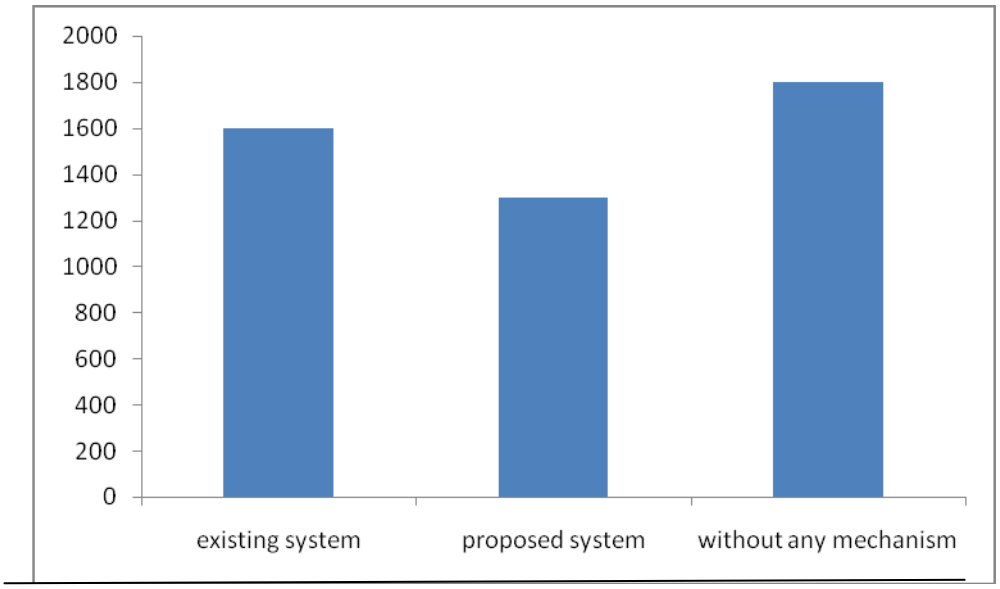

Fig 6.3 : User Data Storage3 Graph

In existing system, we got value like 1599.17. Whereas, in proposed system we got values like 1300. But we got value like 1800 without any mechanism.

7. Conclusion

This paper gives a vital review and heading for the enhanced Cloud Computing Adoption Framework in which the accentuation is on the report on security arrangement, advancements and strategies utilized. The security proposal and updates can help associations building and offering better ensured administrations. However, the storage utilization in cloud is not effective. To overcome this problem, in our proposed block-level storage approach, we have considered hash tables and id's of cloud user's at the cloud storage provider. Each client maintains its hash tables for storing and retrieving the data from storage cloud along with the user authentication. Eventually, our proposed approach can identify the same data of multiple users or same user and it stores in one location, instead of storing multiple locations. Our results prove that block storage can effectively utilize in CCAF framework compare to existing CCAF framework and with replicated mechanism.

8. References

[1] SHA hash functions - Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/SHA1#Description_of_the_algorithms

[2] Wade Trappe, Lawrence C. Washington. 2006. *Introduction to Cryptography with Coding Theory*. New Jersey: Pearson Prentice Hall.

[3] R. Rivest MIT Laboratory for Computer Science and RSA Data Security, Inc. Internet RFC(1320) April 1992.

[4] Chang, V., Walters, R. J. & Wills, G., 2013 b. Cloud Storage and Bioinformatics in a private cloud deployment: Lessons for Data Intensive research. In, Cloud Computing and Service Science, Springer Lecture Notes Series, Springer Book.

[5] Chang, V. & Ramachandran, M., Towards achieving Big Data Security with the Cloud Computing Adoption Framework, IEEE Transactions on Services Computing, forthcoming.

DataLossDB.org survey, 2013, accessible on http://datalossdb.org/us_states in 2013.

[6] IBM, 2010. Defining a framework for cloud adoption, technical report.

[7] Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I., 2010, July. Cloud migration: A case study of migrating an enterprise it system to iaas. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 450-457).

[8] Chang, V., Li, C. S., De Roure, D., Wills, G., Walters, R. J., & Chee, C., 2012. The financial clouds review. Cloud Computing Advancements in Design, Implementation, and Technologies, 125.