International Journal of Engineering & Technology, 7 (1.1) (2018) 607-611

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm

S. Naveen Kumar[1]*, K. Nirmala[2]

[1]Research Scholar, University of Madras, Chennai, India
[2] Research Supervisor, Dept. of Computer Science, Quaid-E-Millath College for Women, Chennai, India
**Corresponding author Email: naveensoupati@gmail.com*

Abstract

Presently a-days Cloud registering is rising field in light of its Performance, high accessibility, easily. Information store is principle future that cloud benefit gives to the huge association to store tremendous measure of information. Yet at the same time numerous associations are not prepared to execute distributed computing innovation since absence of security. So the principle goal of this paper is to understand the security issues and to anticipate unapproved access in distributed storage, it should be possible with the assistance of an effective validation strategy by utilizing cross breed verification calculation to give security of the information in cloud and guarantee amending code to keep up the nature of administration. In any case, solid client confirmation that confines illicit access to the administration giving servers is the foremost prerequisite for securing cloud condition

Keywords: *Cloud Computing, Data Storage, Cloud Security, Blowfish Algorithm, Ensure Correcting Code*.

1. Introduction

Distributed computing is a whole new innovation. It is the advancement of parallel figuring, appropriated processing matrix registering, and is the blend and development of Virtualization, Utility figuring, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) [1]. Cloud is a similitude to portray web as a space where figuring has been pre introduced and exist as an administration; information, working frameworks, applications, stockpiling and handling power exist on the web prepared to be shared. To clients, distributed computing is a Pay-per-Use-On-Demand mode that can helpfully get to shared IT assets through the Internet. Where the IT assets incorporate system, server, stockpiling, application, administration et cetera and they can be sent with much fast and simple way and slightest administration and furthermore connections with benefit providers.[2]

Distributed computing would much be able to enhance its accessibility assets and claims numerous favorable circumstances over other registering methods. Clients can utilize the IT framework with Pay-per-Use-On-Demand mode; this would profit and spare the cost to purchase the physical assets that might be empty. More data on people and organizations is put in the cloud; concerns are starting to develop about exactly how safe a situation it is? Issues of distributed computing [3] can outline as takes after: Privacy, Reliability, Legal Issues, Compliance, Freedom, and Long-Term Viability.

Distributed computing can give unbounded registering assets on request because of its high adaptability in nature, which takes out the requirements for Cloud specialist organizations to prepare on equipment provisioning. Numerous organizations, for example, Amazon, Google, Microsoft et cetera, quicken their paces in creating distributed computing frameworks and upgrading its administrations giving to a bigger measure of clients.

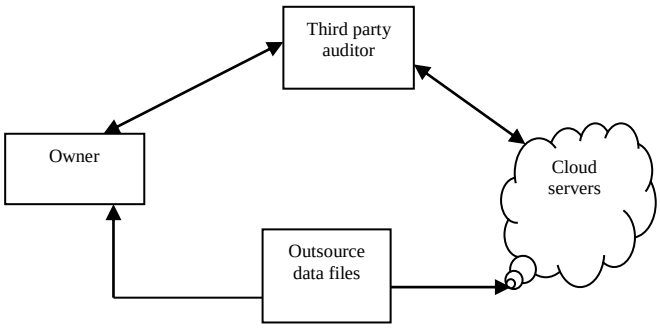

Fig. 1: System architecture of cloud security

This confirmation assaults can be effortlessly happens in the cloud situations. The assailants effectively focus on the servers by these sorts of confirmation assaults [4]. The aggressors focus on the instrument that is taken after client. The component utilized for validation is caught and assailants and tries to get to the private data. They utilize distinctive encryption and unscrambling system to exchange the information as more private. The specialist organization stores the key estimation of clients and must be approved before going to get to an administration. This issue emerges when utilizing a basic validation component, for example, basic username and secret word. In excess of one validation system must be set up in the situations. The auxiliary confirmation system must be utilized and furthermore utilize propelled validation instrument must be utilized to dodge these sorts of assaults. Propelled validation assaults, for example, one time watchword, virtual consoles, site key and so on.

In this paper, we research the security and protection worries of ebb and flow distributed computing frameworks gave by a measure of organizations. As distributed computing alludes to both the applications conveyed as administrations over the Internet and the frameworks (i.e., the equipment and frameworks programming in the server farms) that give those administrations. In light of the examination security and protection concerns gave

by organizations these days are not satisfactory, and therefore result in a major obstruction for clients to adjust into the distributed computing frameworks.
Thus, more worries on security issues, for example, accessibility, secrecy, information respectability, control, and review et cetera, ought to be considered.

2. Literature survey

In 2009, Dmitriy Kuptsov had proposed a two-level circulated verification engineering for remote systems. Versatile hosts are utilizing the Host Identity Protocol (HIP) to associate with the inheritance Internet has through administrator's WLAN. The framework incorporates an administrator particular intermediary server and a disseminated firewall running specifically on WLAN APs. Creators had executed the framework by reflashing the firmware of two distinctive AP models with Linux-based Open-WRT dispersion.
In 2010, Chia-Sheng Tsai had composed a framework that uses a Bluetooth cell phone to open entryways in a completely programmed process with the likelihood to reconfigure the framework to work in self-loader mode to get the endorsement of the client in the event that he input a PIN code as extra security strategy. The plan satisfies the necessity as characterized with quick and secured dispersion of the keys contrasted with the physical keys with least conceivable prerequisites for the equipment, sensible power utilization and support for custom fitted customized keys. A verification convention, a key circulation and a key renouncement technique were proposed.
Tien-Ho Chen et al., (2011) proposed an elliptive bend crypto framework dynamic based plan for shared validation in distributed computing for remote gadgets. This plan is more secured to validate remote servers and clients for distributed computing. It comprised of three stages instatement stage, client enlistment stage and common verification with key understanding stage. This plan gives security against pantomime assault, insider assault, outside assault and common verification.
Mahmood Khalil Ibrahim et al. (2012) proposed a zero information verification convention by altering diifie hellmann key trade calculation. Two variants of the proposed convention are displayed which tackles the issue of man in center assault in D-H key trade calculation. The form 1 is as yet helpless against man in center assault. To shield the proposed calculation from this assault, variant 2 gives shared verification to demonstrate that the server is straightforward. Investigation of the convention demonstrates that it fulfills the ZKP properties and oppose against different assaults like discrete logarithmic assaults and man in the center assaults.
Dinesha et al., proposed a model in (2013) which depends on strict verification framework by presenting multi-level confirmation strategy which creates and verifies the secret word in different levels to get to the cloud administrations. The confinement of these strategies is they utilize a similar secret word at various level of verification.
Tumpe Moyo et al.,(2014) proposed to test the obstacle shielding associations from receiving cloud (with a specific spotlight on the security issues).The overview respondents fundamentally favored the utilization of half breed or private cloud. The overview comes about demonstrate the prominence of cloud innovation. security is as yet an issue inside distributed computing however the above research shows this is taking a positive turn and is enormously enhancing as the cloud innovation and reception creates.
Majid Bakhtiari et al.,(2015) concentrated on the security control force at continuous clog level of the framework. With the control of different security quality, a similar part had distinctive actuated licenses. They tackled the issue of the securing the protection of clients' consents. the calculation had similitudes in the delicate degree of authentication assaults and punishments. At the point when non approved client assaulting, the client's trusted level and trusted esteem would be hard to come back to the past level, along these lines they think to oppose verification assaults. They kept up different variables steady and changed just a factor, the delicate level of vindictive assaults and punishments would be facilitated, and the affectability and punishments would change with the difference in the significance level of different elements.
Mohamed M. Zarad et al., (2016) proposed an effective and provably secure confirmation system to give a real client the privilege to get to and deal with the cloud assets. It gives a helpful on request arrange access to a pool of shared administrations and assets by means of open systems. So undertakings can utilize the accessible administrations and assets to create, host, and run benefits over their foundation adaptably whenever, anyplace with insignificant administration endeavors. The necessity of endorsement expert for this calculation requires a huge stockpiling limit and check of authentications backs off the framework execution because of multifaceted nature of key creation since this calculation is restricted by the prime and productivity of creating primes which require a great deal of counts that back off the encryption and decoding process.

3. Problem statement

- There are different approaches issues and dangers in distributed computing innovation which incorporate protection, isolation, stockpiling, unwavering quality, security, limit and that's just the beginning. Be that as it may, most critical among these to concern is security and how specialist organization guarantees it to keep up.
- Generally distributed computing has a few clients, for example, normal clients, the scholarly community and undertakings who have distinctive inspirations to move to cloud.
- For undertakings most essential issue is likewise security yet with various vision. Along these lines, we for the most part focus on information security of distributed computing utilizing encryption calculation utilizing specific proposed design.
- There are numerous physical and some other assault on information that pulverize information on server and this can be overwhelmed by dissipating the information on in excess of one server rather than one server. But this by itself not take care of issue totally in light of the fact that, information put away in scrambled mode utilizing encryption scratch. The aggressors assault on scratch and might be hack the information.
- So, it is critical to utilize the productive key administration calculations amid the confirmation assault.

4. Research methodology

To guarantee the security and trustworthiness for cloud information stockpiling under the previously mentioned foe demonstrate, we expect to plan proficient systems for dynamic information check and task. This should be possible by utilizing three stages, order stage, verification stage, stockpiling stage. Our proposed proficient key administration validation calculation is based of blowfish calculation with homomorphic based key age process.

4.1. Requition phase

To guarantee the security and trustworthiness for cloud information stockpiling under the previously mentioned foe demonstrate, we expect to plan proficient systems for dynamic information check and task. This should be possible by utilizing three stages, order stage, verification stage, stockpiling stage. Our proposed proficient key administration validation calculation is based of blowfish calculation with homomorphic based key age process.

4.2. Authentication phases

At the point when a client needs to get to the online Cloud Service, acknowledge to native kill the Login Program. This progression can utilize acknowledged web based business or included casework which acknowledge as of now profoundly outright the client's enlistment, for example, symmetric key-based asserting and affirmation login check, or through a One-Time Password. After the client's login has been favorably confirmed, if the System requires candidate counsel from the client, it sends an interest for guidance to the Storage Service System. In this progression, the System transmits the client ID to the Storage Service System zone it scans for the client's information.

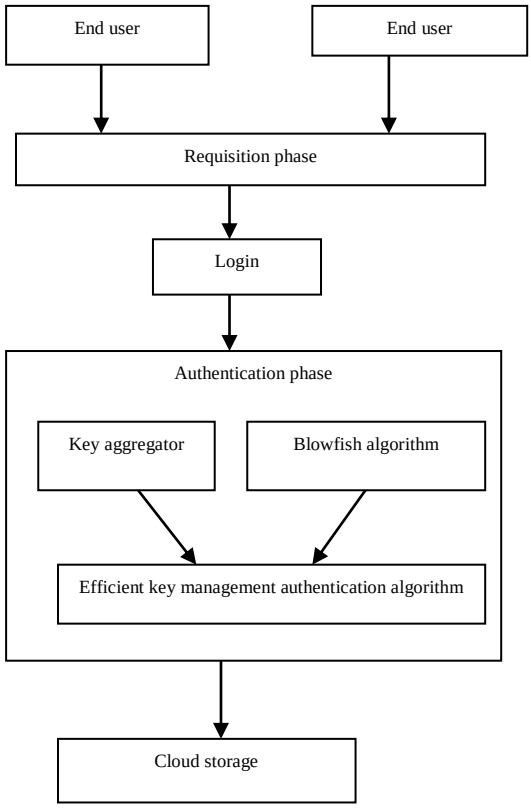

Fig. 2: Proposed system architecture

4.2.1. Efficient key management authentication algorithm:

Blowfish is symmetric square figure calculation encodes piece information of 64-bits at once. This calculation is isolated into two sections.

a. Key-generation
b. Sub keys generation
c. Key aggregation
d. Data Encryption/decryption

(a)Key generation:

Blowfish utilizes countless. These keys must be pre-processed before any information encryption or decoding.
The P-exhibit comprises of 18 32-bit subkeys: P1, P2,..., P18.
There are four 32-bit S-boxes with 256 passages each:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..., S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,..., S4,255.

(b) Generating the Subkeys

The subkeys are ascertained utilizing the Blowfish calculation:
1. Instate first the P-exhibit and after that the four S-boxes, all together, with a settled string. This string comprises of the hexadecimal digits of pi (less the underlying 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, and so on.

2. XOR P1 with the initial 32 bits of the key, XOR P2 with the second 32-bits of the key, et cetera for all bits of the key (perhaps up to P14). Over and again go through the key bits until the whole P-cluster has been XORed with key bits. (For each short key, there is no less than one equal longer key; for instance, if A will be a 64-bit key, at that point AA, AAA, and so on., are equal keys.)
3. Scramble the every one of the zero string with the Blowfish calculation, utilizing the subkeys depicted in steps (1) and (2).
4. Supplant P1 and P2 with the yield of step (3).
5. Scramble the yield of step (3) utilizing the Blowfish calculation with the altered subkeys.
6. Supplant P3 and P4 with the yield of step (5).
7. Proceed with the procedure, supplanting all passages of the P exhibit, and after that every one of the four S-encloses arrange, with the yield of the persistently changing Blowfish calculation. Altogether, 521 cycles are required to create all required sub keys. Applications can store the subkeys instead of execute this induction procedure different circumstances.

(c)Key aggregation

The encryption of messages in the key conglomeration process is done under a specific open key as well as per an identifier of the figure content called class .A figure content class is a self-assertive whole number characterizing an order as made by the information proprietor under which the plain content is to be encoded .Thus ,the figure writings are arranged into various classes .The key proprietor possesses an ace mystery called ace mystery key ,which can be utilized to extricate mystery keys for various classes .The key that is separated can be a total key which joins the energy of numerous mystery keys permitting the unscrambling of in excess of one figure content with a similar total key . The sizes of figure content ,open key, ace mystery key ,and total key in the plan are all of consistent size.This gives extraordinary time and security points of interest over the one key for every demand for document and one key for all records conspires separately

(d)Encryption

It is having a capacity to emphasize 16 times of system. Each round comprises of key-subordinate stage and a key and information subordinate substitution. All tasks are XORs and augmentations on 32-bit words. The main extra tasks are four filed cluster information query tables for each round.
Calculation for Blowfish Encryption
Separation x into two 32-bit parts: xL, xR
For I = 1to 16:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR
These keys calculation work we are thinking about has a place with a group of all inclusive hash work, saved the encryption properties, which can be impeccably coordinated with the check of deletion coded information. One next to the other, it is indicated checking the capacity accuracy and in addition distinguishing getting into mischief server.

5. Performance Analysis

Practically, based on three parameters we can say that our proposed work is better and these parameters are:

- Execution time
  - Encryption Time
  - Decryption Time
- Avalanche effect

Execution time

The aggregate time taken by a procedure to change over plain content into figure content is called encryption time or figure content to plain content is called decoding time. Table 1 and Figure 5 is demonstrating the examination of encryption time of proposed work and Table 2 and Figure 6 is demonstrating the investigation of unscrambling time of proposed work.

Table 1: Encryption Time Analysis

Size (KB)	Efficient key management authentication algorithm	AES algorithm
8,232	954	1025
389	23	55
36	11	20
2785	389	370
Average time	243	365.9

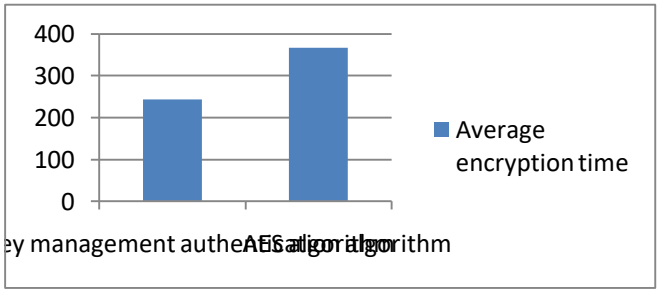

Fig. 3: Encryption time analysis

Table 2: Decryption Time Analysis

Size (KB)	Efficient key management authentication algorithm	AES algorithm
8,232	200	434
389	110	265
36	13	34
2785	21	394
Average time	113.5	200.3

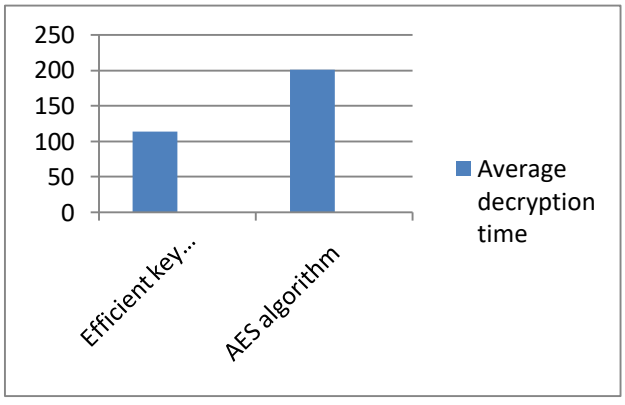

Fig. 4: Decryption time analysis

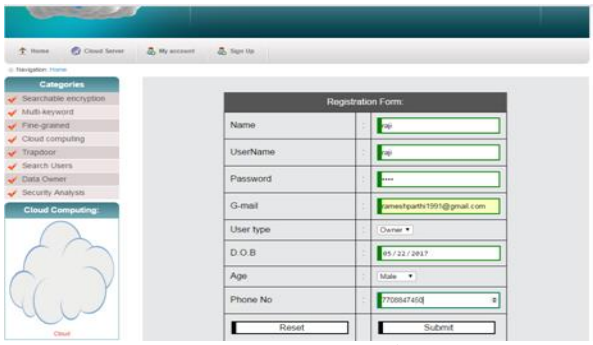

Fig. 5: Owner registering in cloud for accessing

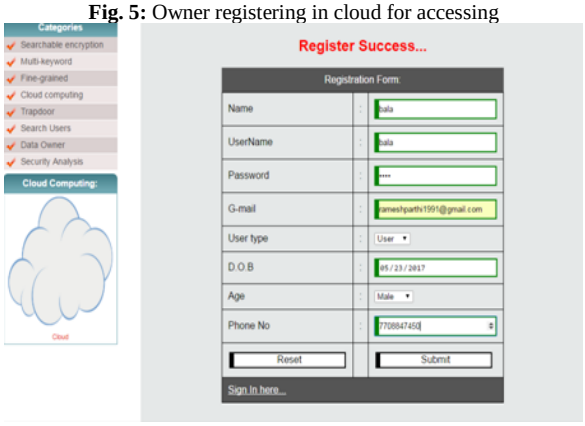

Fig. 6: User registering in cloud for accessing

Figure 5 and 6 shows the registration phase in the cloud by both the owner and user. They are registered with separate password and username.

Fig. 7: Authentication process

Here the username and password is provided with user type and secret key. This key is symmetric

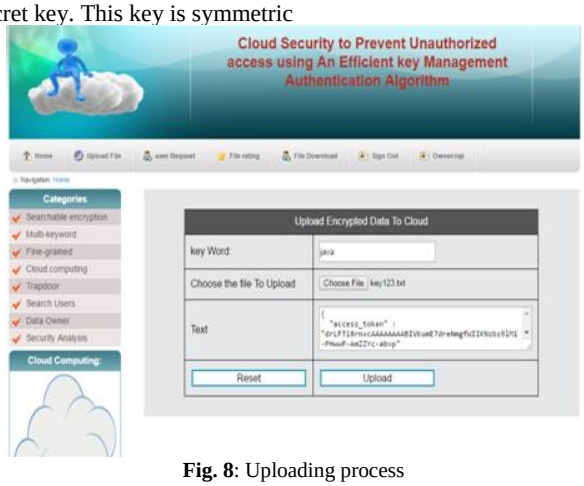

Fig. 8: Uploading process

The file which hast be store in the cloud in done as indicated in the figure-8

Fig. 9: Rating the size of files

Fig. 10: Downloading process

Before the file being uploaded the size of the file has to be known that is indicated in figure 9 and the downloading process in denoted in figure-10

Avalanche effect

In cryptography, the torrential slide impact [19] is a most noteworthy property for piece figuring and hash work calculations. The torrential slide impact situation is satisfied in following conditions:

In the event that the yield changes significantly (e.g., a large portion of the yield bits flip) causes a minor change in input (e.g., flipping a solitary piece).

In square figures, such a little change in either the key or the plaintext should grounds to a solid change in the figure content.

The above states of torrential slide impact enable little changes to spread quickly through cycles of the calculation, such that all of the yield ought to rely upon all of the contribution before the calculation ends.

Torrential slide Effect Formula is given beneath:

Torrential slide Effect = (Number of progress bits in figure content)/(Number of bits in figure content)

From the above outcomes examination it can obviously observe that the proposed strategy has better Avalanche Effect and encryption/unscrambling time than existing procedure and consequently can be consolidated during the time spent encryption/decoding of any plain content or on any key esteem. Likewise, in any case it is additionally obvious from above talk that, by applying proposed strategy to the content of various sizes high piece distinction is gotten as contrast with various other existing. Thus terms of execution time (Encryption Time and Decryption Time) of the proposed method have low when contrasted with existing procedure.

6. Conclusion

Thus the proposed Efficient key management authentication algorithm using blowfish algorithm to provide security of the data in cloud and ensure correcting code to maintain the quality of service. The cloud is support for data redundancy means clients can insert, delete or can update data so there should be security mechanism which ensure integrity of data. This paper also secures the data while the misbehaving of the server arises. The performance analysis validate the proposed work by means of verifying the execution time for both encryption and decryption, key analysis and Avalanche Effect of the proposed technique is better when compared to existing techniques.

References

[1] Dillon T, Wu C & Chang E, "Cloud Computing: Issues and Challenges", *24th IEEE International Conference on Advanced Information Networking and Applications(AINA)*, (2010), pp.27-33.

[2] Zhou MQ, Zhang R, Xie W, Qian WN & Zhou A, "Security and Privacy in Cloud Computing: A Survey", *Sixth International Conference on Semantics, Knowledge and Grids(SKG)*, (2010), pp.105-112.

[3] Yang JF & Chen ZB, "Cloud Computing Research and Security Issues", *IEEE International Conference on Computational Intelligence and Software Engineering (CiSE)*, (2010), pp.1-3.

[4] Zhang S, Zhang SF, Chen XB & Huo XZ, "Cloud Computing Research and Development Trend", *Proceedings of the Second International Conference on Future Networks*, (2010), pp. 93-97.

[5] Kuptsov D, Khurri A & Gurtov A, "Distributed user authentication in Wireless LANs", *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops*, (2009), pp.1-9.

[6] Tsai CS & Hung CI, "An Enhanced Secure Mechanism of Access Control", *Second International Conference on Communication Systems, Networks and Applications (ICCSNA)*, pp.119-122, (2010).

[7] Chen TH, Yeh HL & Shih WK, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing", *IEEE conf. on Multimedia and Ubiquitous Engineering*, (2011).

[8] Ibrahem MK, "Modification of Diffie-Hellman key exchange algorithm for Zero knowledge proof", *future Communication Networks (ICFCN)*, (2012), pp.147-152.

[9] Dinesha H & Agrawal V, "Multi-level authentication technique for accessing cloud services", *International Conference on Computing, Communication and Applications*, (2013), pp.1-4.

[10] Moyo T & Bhogal J, "Investigating Security Issues in Cloud Computing", *Eighth International Conference on Complex, Intelligent and Software Intensive Systems, (2014)*.

[11] Babaeizadeh M, Bakhtiari M & Mohammed AM, "Authentication Methods in Cloud Computing: A Survey", *Research Journal of Applied Sciences, Engineering and Technology*, (2015).

[12] Zarad MM, Abdel-Hafez AA & Hassanein AH, "Secure and Efficient Authentication Scheme for Cloud Computing", *International Journal of Computer Applications*, (2016).