Research Article

Efficient Data Storage Security Analysis Using Randomized Algorithm in Cloud

C. Saranya Jothi[a], and S. Ranathive[b]

[a] Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr. Sagunthala R& D Institute of science and Technology,
Avadi, Chennai-62, India
[b]Department of Computer Science and Engineering,
Vel Tech Rangarajan Dr. Sagunthala R& D Institute of science and Technology, Avadi, Chennai-62, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Database re-appropriating is a common circulated registering perspective that empowers data owners to misuse its on-request accumulating and computational assets. The guideline challenge is keeping up the data arrangement concerning entrusted parties. We propose a combination of triple randomized algorithms namely 3DES, AES, Blowfish. The data owner can select between the encryption methods which is suitable. As each of the algorithms takes a different block size as input and also has various key sizes. Another issue that arises is the redundancy of data. When many copies of identical data are stored, the storage size decreases, and large storage space is required. Here data reduplication technique, which is used to identify duplicate files using the hash code value method for better storage space.

Keywords: Encrypted Algorithm, Blowfish, cloud storage, AES, 3DES.

1. Introduction

The information is transferred into outsider specialist organizations by the associations because of its expansion. The capacity cost and the computational assets are diminished by enabling the information proprietors to transfer the information to databases. For a less cost, associations with a constrained asset can transfer their enormous volumes of information to an outsider specialist organization and use their progressively versatile capacity just as computational power. Be that as it may, a classification and uprightness issue emerges because of the way that the information is constrained by outsiders thus raises basic security issues. Information classification necessitates that information isn't unveiled to entrusted clients and information honesty guarantees that information isn't changed before being handled by the server. As of late, various areas, for example, the database and the cryptography network have investigated the issue of questioning scrambled information at the entrusted specialist co-op. This redistributing of information cuts down both speculation cost and operational costs for colossal enterprises [10]. In the meantime, redistributing involves that clients lose essential control of their information and activities performed on the information [9]. This thusly infers the information is powerless to security reduced volumes and the cost of large storage systems.

We defeat the issue of security in the cloud, which is important to be kept safe from an untrusted third party and keep the data hidden from service providers. Secure communication between the up loader and the user can be achieved by providing much higher security by using multiple encryption algorithms.

The AES algorithm uses a square size of 128 bits, by knowing the specific algorithm it is very likely to be breached by brute-force technique giving no time to secure the data. To overcome this combo of randomized algorithms namely 3DES, AES, Blowfish are used which makes cryptanalysis difficult [6]. The usage of these combined algorithms provides better security.

The dynamic nature of the cloud is storage, with the increasing data and reduced volumes and the cost of large storage systems. To reduce the problem of redundancy a data de-duplication technique has been brought to improve storage efficiency in cloud storage. At the point when numerous duplicates of fundamentally the same as or even indistinguishable information are put away, the hash code value method is used to identify duplicate data. The aim is to combining cryptography with cloud computing in an innovative way to improve the security of the whole system.

2. Related Works

A framework that accomplishes privacy and enables square dimension reduplication at the equivalent time. Our framework is manufactured over merged encryption [4]. Information is put away in a database utilizing a strong and secures encryption strategy, (for example, Progressed Encryption Standard (AES) [5]. The cloud maintained by various service providers provide their service to users for storage and sharing purposes where the users can upload their data and retrieve them when needed, these data can also be shared among other users in remote places and get the files required [7]. The data owner uploads the files for sharing to the cloud in an encrypted format which is stored with the cloud on the maintenance of the service provider. The files from many users are uploaded and are made visible so that other users can locate the necessary files [8]. The data user who is in need require the file views them and download the required files with the key provided during the upload. In [1] Cloud-DLP, a straightforward and adaptable methodology for undertakings to consequently purify delicate information in pictures and records with the different program based cloud applications. Cloud-DLP is sent as a web passage inside the premises of an endeavor utilizing JavaScript infusing strategies and profound learning techniques to disinfect delicate reason information.

The review plan [2] of the assigned specialist actualizes a lightweight figuring for the gathering individuals however; it overlooks the security dangers between the gathering individuals and the operators. By presenting Hash graph innovation and planning a third party medium the executive's system, a lightweight secure reviewing plan for shared information in distributed storage is proposed, which accomplishes security the board of the gatherings and a lightweight figuring for the gathering individuals.

The issue of extra room can be settled by utilizing Cloud Storage Service [3] that will in general give a huge extra room to the nearby end clients. As CSS doesn't have its own stockpiling to make sure about the client's information, it presents numerous information security challenges in the distributed computing worldview. In any case, some conventional frameworks don't satisfy the security prerequisites for endeavors and shoppers in Service Level Agreements. This remaining parts a critical bottleneck for administration selection. The conversation of late improvements on the security of the distributed computing worldview is given in this exploration work.

3. Proposed System

In this, the data owner uploads the file to the cloud which is readily available to be shared. When the file is being uploaded it is checked for redundancy, if the same file already exists then the file isn't uploaded thus in-turn saving space. The files are encrypted in a randomized format consisting of the algorithms AES, Blowfish, and Triple-DES. The user who needs these files requests the files to download. The download request is sent to both the data owner and the admin. Both after receiving the request respond to it and two keys are generated which are automatically sent to the data user. When the filename, user key, data uploaded key matches the file is available for downloaded are shown in Fig.1

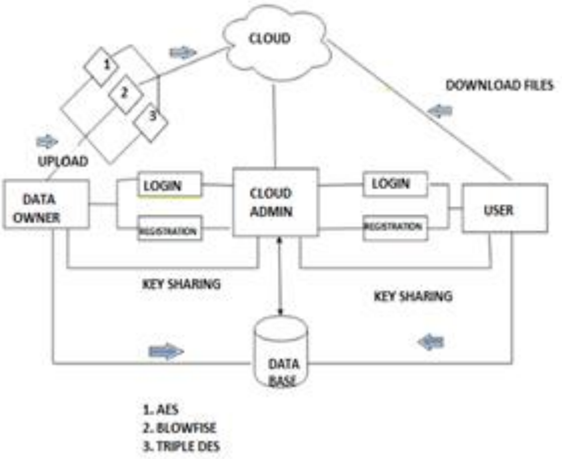


Fig.1. Proposed System

A. Registration Details

The users need to register themselves with appropriate credentials which will be later useful in logging in and performing operations such as uploading and downloading the files are shown in fig.2. This model has been made for client verification reasons. In this login page, Approved clients can login with their substantial accreditations. The enlisted subtleties will be put away into the database and will be to verify while logging time. It will confirm every single client data subtleties. On the off chance that those subtleties are doesn't coordinate with database subtleties, at that point it will give a blunder message and it will demonstrate the enrollment page naturally. In this way, here we are avoiding the illicit clients and giving more observation to our application.

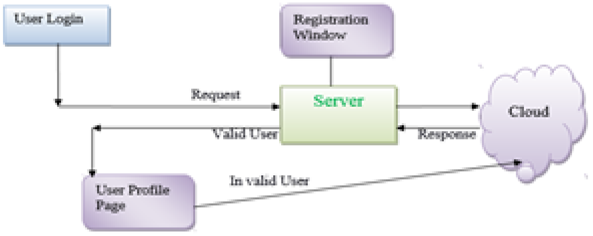


Fig.2. Registration Details

B. Data Upload

The data owner uploads the files which are ready to be shared in an encrypted format. This information will be transferred to the cloud. In, multi-target reinforcement will be reduplication examination and put away into the cloud applications is proposed. In light of a lot of target requirements and loads characterized by the client, the framework endeavors to locate a suitable Pareto arrangement in the locale of enthusiasm for the clients. It is modified and dissected for four destinations: make range, cost, unwavering quality, and vitality are shown in fig.3.

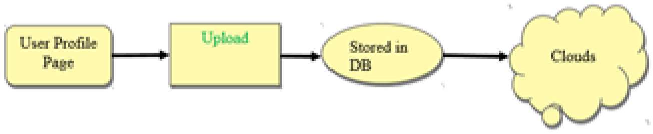


Fig.3. Data upload

C. View and Analysis

In this, the uploaded files will be viewed for confirmation and analysis use. When the files are successfully uploaded by proper analysis than the user and finally request the wanted file from the uploaded file are shown in fig.4.

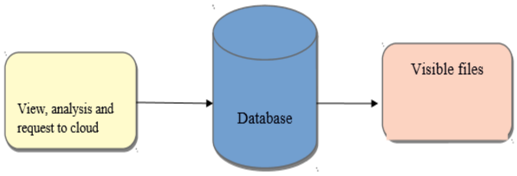


Fig.4.View and Analysis

D. Key Request

In this, the allocation of resources for users which are processed after the scheduling process. The implementation of the make spam & monitoring cost of the process which involves a dynamic process. By using the strategy profile of the user process we will allocate the time based on the tasks which are performed by the user. Here, we will also introduce a key method that is going to involve a reverse mechanism to the user for his choices shown in fig.5.

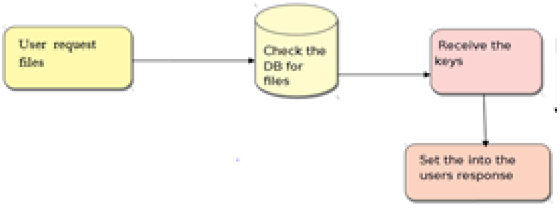


Fig.5. key Request

E. Deliver Product (Data)

The data user requests the file for download. The file is checked in the database for availability, if available then the owner gets a request followed by the admin. The responses from both are the keys that are automatically allocated and then the filename and the other two keys are verified. On successful verification, the files are available for download shown in fig 6.

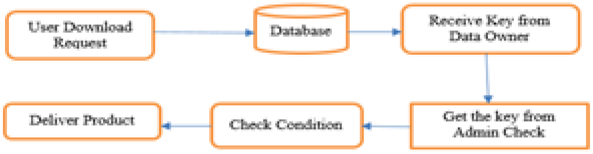
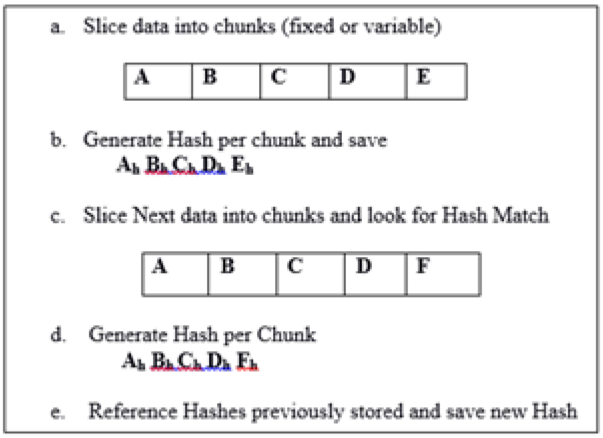


Fig.6. Deliver product

4. Technique Used

A. Data De-duplication

Information de-duplication, as often as possible called savvy pressure or single-event stockpiling, is a methodology that executes abundant copies of data and reduces stockpiling overhead. Information de-duplication techniques ensure that only a solitary unprecedented event of data is hung on limited media, for instance, plate, burst, or tape. Redundant data squares are replaced with a pointer to the exceptional data copy. Thusly, Data de-duplication eagerly lines up with consistent fortification, which copies only the data that has changed since the past support is shown in fig 7.



a. Slice data into chunks (fixed or variable)

A	B	C	D	E

b. Generate Hash per chunk and save
A_h B_h C_h D_h E_h

c. Slice Next data into chunks and look for Hash Match

A	B	C	D	F

d. Generate Hash per Chunk
A_h B_h C_h D_h F_h

e. Reference Hashes previously stored and save new Hash

Fig.7. Data De-duplication

5. Implementation

Data will be uploaded into the cloud. In a multi-objective backup will be reduplication analysis and stored into the cloud. After uploaded files will be viewed for confirmation and analysis use. When the files are successfully uploaded by proper analysis than the user and finally request the wanted file from the uploaded file. The request is sent to the data owner and the admin who responses to the request shown in fig.8.

Fig. 8.View and Analysis

In this the allocation of resources for users which are processed after the scheduling process. The implementation of the make spam & monitoring cost of the process which involves a dynamic process. By using the strategy profile of the user process we will allocate the time based on the tasks which are performed by the user. Here, we will also introduce a key method that is going to involve a reverse mechanism to the user for his choices shown in fig.9.

Fig.9. Key Request

The data user requests the file for download. The file is checked in the database for availability, if available then the owner gets a request followed by the admin. The responses from both are the keys that are autocratically allocated and then the filename and the other two keys are verified. On successful, verification the files are available for download shown in fig.10.

Fig.10. Deliver Product (Data)

TABLE I. TEST CASE

Test case Id	Testing	Expected Result	Actual Result	Status
01	Registration	Successfully Registered	Successfully Registered	Pass
02	Login	Login Successful -correct Credentials Login Unsuccessful -Incorrect Credentials	Login Successful Error Message	Pass Pass
03	Multi-Objective Backup	-File Upload -Duplication Detection	Successfully Uploaded Duplicate File Detected	Pass Pass
04	Data View	File available	File Visible	Pass
05	Send Request	Request the data owner and admin	Request Successful	pass
06	Response	-Data Owner Response -Admin Response	-Accepted -Rejected -Accepted -Rejected	Pass Pass Pass pass
07	Key Delivery	Key Delivery	Key not Delivery	Fail

6. Conclusion And Future Enhancement

Database re-appropriating is a mainstream worldview of distributed computing. In this work, we are attempting to accomplish a harmony between information privacy at the server and productive inquiry preparation. We encode utilizing randomized calculations. Next, we make it increasingly secure by applying encryption to the changed information. We characterize a few assault models and demonstrate that our plan gives strong protection from them. This allows an agreement between the security of data and brisk response time as the inquiries are set up on mixed data at the cloud worker. Also Besides, we contrast and existing methodologies on huge datasets and demonstrate that this methodology decreases the normal inquiry. In future enhancement, the size of the uploaded files can be expanded and they can share the files in various formats. Furthermore, the security can be increased by including many more encryption standards expanding the possibilities.

References

1. Peiyi Han, Chuanyi Liu, Jiahao Cao, Shaoming Duan, Hezhong Pan, Zekun Cao, Binxing Fang, " CloudDLP: Transparent and Scalable Data Sanitization for Browser-Based Cloud Storage", in IEEE Access, 2020, Volume: 8.
2. Junfeng Tian, Xuan Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage", in IEEE Access2019, Volume: 7.
3. B S Vamsi Krishna, S Sreenivasa Rao, MHM Krishna Prasad, " Security on Data Auditing Protocols for Cloud Storage Data" 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE.
4. Mihkhali Babenko, Nikolay Chervyakov,Andrei Tchernykh, Nikolay Kucherov, Maxim Deryabin, Gleb Radchenko, Philippe O A Navaux, Viktor Svyatkin, “Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack”, Young Researchers in Electrical and Electronic Engineering, 2018 IEEE Conference of Russian.
5. Yan Yang, Xingyuan Chen, Hao Chen, Xuehui Du, “ Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing ,”2018 IEEE Access (Voume:6).
6. Srijita Basu, Arjun Bardhan Koyal Gupta, Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu, Saunak Chaudhary, Pritika Sarkar“Cloud computing security challenges & solutions-A survey”, 2018 IEEE Computing and Communication Workshop and Conference (CCWC).
7. Xiaofeng Chen, Willy Susilo, “Secure and Efficient Cloud Data Deduplication with Randomized Tag”, IEEE Transactions on InformationForensics and Security(Volume: 12, Issue: 3, March 2017).
8. Ayesha M. Talha, Ibrahim Kamel, “Facilitating Secure and Efficient Spatial Query Processing on the Cloud”, 2017 IEEE Transactions on Cloud Computing.

9. Vishalakshi N S, S.Sridevi, “Survey on Secure De-duplication with Encrypted Data for Cloud Storage”, 2017, Vol 4, Issue 1.
10. Vinodary Thumar,Dr.Vipul Vekariya “A Technical Review on mobile cloud computing Security Issues and Research Challenges", in IEEE Access Volume 4,Issues 10,October 2017.