© 2019 IJSRST | Volume 6 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : https://doi.org/10.32628/IJSRST196250

Proficient Justification of Data Accuracy for Cloud Storage Using Dual Protection

Deepika. N[1], Durga. P[1], Gayathri. N[1], Murugesan. M[2]
[1]UG Scholar, Dhanalakshmi College of Engineering, Tamilnadu, India
[2]Associate Professor, Dhanalakshmi College of Engineering, Tamilnadu, India

ABSTRACT

The cloud security is one of the essential roles in cloud, here we can preserve our data into cloud storage. More and more clients would like to keep their data to PCS (public cloud servers) along with the rapid development of cloud computing. Cloud storage services allow users to outsource their data to cloud servers to save local data storage costs. Multiple verification tasks from different users can be performed efficiently by the auditor and the cloud-stored data can be updated dynamically. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. In our system we are using the own auditing based on the token generation. Using this key generation technique compare the key values from original keys we can find out the changes about the file. A novel public verification scheme for cloud storage using in distinguishability obfuscation, which requires a lightweight computation on the auditor and delegate most computation to the cloud. Not only stored also the content will be encrypted in the cloud server. If anyone try to hack at the cloud end is not possible to break the two different blocks. The security of our scheme under the strongest security model. They need first decrypt the files and also combine the splitted files from three different locations. This is not possible by anyone. Anyone can download the files from the server with file holder permission. At the time of download key generated (code based key generation) and it will send to the file owner. We can download the file need to use the key for authentication and some other users want to download file owner permission is necessary.

Keywords : Key Generation Technique, File Auditing, Token Generation, Public Verification Key.

I. INTRODUCTION

Distributed computing has been envisioned as the accompanying creation information development (IT) plan for endeavors, due to its broad summary of unparalleled inclinations in the IT history: on-ask for self-advantage, inescapable framework get to, zone self-choosing resource pooling, quick resource adaptability, use based assessing and transference of peril. As an aggravating development with huge consequences, distributed computing is changing the specific method for how associations use information advancement. One fundamental piece of this standpoint changing is that data are being united or outsourced to the. From customers' view, including together individuals and IT tries, securing data remotely to the in a versatile on-ask for strategy bring engaging focal points: landing of the weight for storage space organization, vast data access with put self-sufficiency, and avoidance of advantages costs on hardware, programming, and staff frameworks of help, etcetera. While distributed computing make these compensation more captivating than some other time in ongoing memory, it also passes on new and testing security risks to customers' outsourced data. As organization providers (CSP) are part

administrative components, data outsourcing is truly surrendering customer's last control more than the fate of their data.

As an issue of first significance, in spite of the way that the structures underneath the are altogether more powerful and trustworthy than individual enlisting devices, they are still before the broad assortment of both inside and outside risks for data respectability.

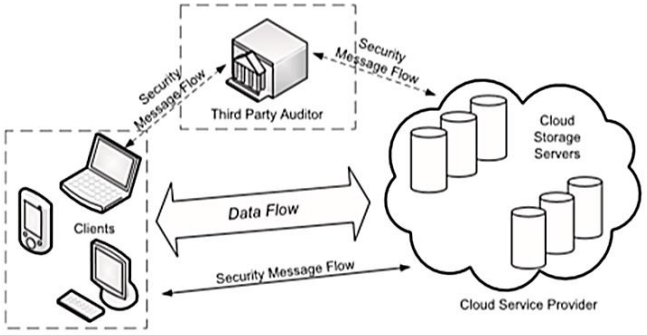


Fig. 1. Cloud data storage architecture.

1.1 SCOPE OF THE PROJECT

As rapid systems and omnipresent Internet get to wind up accessible as of late, numerous administrations are given on the Internet to such an extent that clients can utilize them from anyplace whenever. Information vigor is a noteworthy prerequisite for capacity frameworks. There have been numerous proposition of putting away information over.

1.2 NEED FOR THE PROJECT

As a problematic innovation with significant ramifications, processing is changing the plain idea of how organizations utilize data innovation. One essential part of this outlook changing is that information.

Are being brought together or outsourced to the . From clients' point of view, including the two people and IT ventures, putting away information remotely to the in an adaptable on-request way brings engaging advantages: alleviation of the weight for capacity administration, general information access with area freedom, and evasion of capital consumption on equipment, programming, and work force systems for upkeeps, and so on.

1.3 OBJECTIVE OF THE PROJECT

Specialist organizations (CSP) are separate authoritative elements, information outsourcing is really giving up client's definitive control over the destiny of their information. Thus, the rightness of the information in the is being put in danger because of the accompanying reasons.

Above all else, despite the fact that the foundations under the are substantially more ground-breaking and solid than individualized computing gadgets, they are as yet confronting the wide scope of both inward and outside dangers for information respectability.

Design Goals -- To correctly verify the integrity of shared data with efficient user revocation, our public auditing mechanism should achieve the following properties: (1) Correctness: The TPA is able to correctly check the integrity of shared data. (2) Efficient and Secure User Revocation: On one hand, once a user is revoked from the group, the blocks signed by the revoked user can be efficiently re-signed. On the other hand, only existing users in the group can generate valid signatures on shared data, and the revoked user can no longer compute valid signatures on shared data. (3) Public Auditing: The TPA can audit the integrity of shared data without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

II. LITERATURE SURVEY

ENABLING CLOUDSTORAGE AUDITING WITH KEY-EXPOSURE RESISTANCE

AUTHOR: Jia Yu, KuiRen, Cong Wang, Vijay Varadharajan (2015)

Cloud storage auditing is viewed as an important service to verify the integrity of the data in public cloud. Current auditing protocols are all based on the assumption that the client's secret key for auditing is absolutely secure. However, such assumption may not always be held, due to the possibly weak sense of security and/or low security settings at the client. If such a secret key for auditing is exposed, most of the current auditing protocols would inevitably become unable to work. In this paper, a new paradigm called auditing protocol with key-exposure resilience is proposed. In such a protocol, the integrity of the data previously stored in cloud can still be verified even if the client's current secret key for cloud storage auditing is exposed. We formalize the definition and the security model of auditing protocol with key-exposure resilience, and then propose the first practical solution. The security proof and the asymptotic performance evaluation show that the proposed protocol is secure and efficient.

Advantages -- The integrity of the data previously stored in cloud can still be verified even if the client's current secret key for cloud storage auditing is exposed. The security proof and the performance analysis show that our proposed protocol is secure and efficient.

Disadvantages -- The verification algorithm does not need a secret key from the auditor in an auditing protocol with public verifiability. Therefore, any third party can play the role of the auditor in this kind of auditing protocols.

ENABLING PUBLIC AUDITABILITY AND DATA DYNAMICS FOR STORAGE SECURITY IN CLOUD COMPUTING

AUTHOR: Qian Wang, Cong Wang, KuiRen, Wenjing Lou and Jin Li (2011)

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. Although schemes with private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks.

Advantages -- Private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the

cloud server for correctness of data storage while keeping no private information.

Disadvantages -- It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood.

PRIVACY-PRESERVING PUBLIC AUDITING FOR DATA STORAGE SECURITY IN CLOUD COMPUTING

AUTHOR: Cong Wang, Qian Wang, KuiRen and Wenjing Lou (2010)

In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphism authenticator and random masking to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner.

Advantages -- Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. To support efficient handling of multiple auditing tasks

Disadvantages -- Which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

AUTHOR :Boyang Wang, Baochun Li and Hui Li (2014)

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information—identity privacy—to public verifiers. In this paper, a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud is proposed. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. This results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

Advantages -- The efficiency of verifying multiple auditing tasks is improved by extending mechanism to support batch auditing.

Disadvantages -- Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected, the current design of ours does not support traceability. The data freshness is not proved, while preserving identity privacy.

PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN THE CLOUD

AUTHOR: BoyangWang ,Baochun Li and Hui Li (2013)

With data services in the cloud, users can easily modify and share data as a group. To ensure data integrity can be audited publicly, users need to compute signatures on all the blocks in shared data. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. When a user in the group is revoked, we allow the cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.

Advantages -- The efficiency of user revocation is improved and existing users in the group can save a significant amount of computation and communication resources during user revocation.

Disadvantages -- The auditing mechanism is designed to preserve identity privacy for a large number of users. However, it fails to support public auditing.

PANDA: PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN THE CLOUD

AUTHOR: Boyang Wang, Baochun Li and Hui Li (2015)

With data services in the cloud, users can easily modify and share data as a group. To ensure data integrity can be audited publicly, users need to compute signatures on all the blocks in shared data. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. A public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud.

Advantages -- When a user in the group is revoked, the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures is allowed. The efficiency of user revocation is improved, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

Disadvantages -- Proofs of Retrievability (POR) and its subsequent work do not support public verification, which fails to satisfy the design objectives.

ON THE KNOWLEDGE SOUNDNESS OF A COOPERATIVE PROVABLE DATA POSSESSION SCHEME IN MULTICLOUD STORAGE

AUTHOR :Huaqun Wang and Yuqing Zhang (2014)

Provable data possession (PDP) is a probabilistic proof technique for cloud service providers (CSPs) to prove the clients' data integrity without downloading the whole data. The existence of multiple CSPs to cooperatively store and to maintain the clients' data is studied. Then, based on homomorphic verifiable

response and hash index hierarchy, a cooperative PDP (CPDP) scheme from the bilinear pairings is presented. This scheme satisfied the security property of knowledge soundness. It shows that any malicious CSP or the malicious organizer (O) can generate the valid response which can pass the verification even if they have deleted all the stored data, i.e., Then, we discuss the origin and severity of the security flaws. It implies that the attacker can get the pay without storing the clients' data. It is important to clarify the scientific fact to design more secure and practical CPDP scheme in Zhu et al.'s system architecture and security model CPDP scheme cannot satisfy the property of knowledge soundness. Then, the origin and severity of the security flaws is discussed. It implies that the attacker can get the pay without storing the clients' data. It is important to clarify the scientific fact to design more secure and practical CPDP scheme in Zhu et al.'s system architecture and security model.

Advantages -- The malicious CSPs can deceive the clients by getting their payments without storing their data. Thus, the clients will be confronted with huge losses when they want to retrieve their data since they do not store the data locally.

Disadvantages -- CPDP scheme does not satisfy the knowledge soundness. It is still an open problem to design secure and efficient CPDP scheme for integrity verification in multi-cloud storage.

IDENTITY-BASED DISTRIBUTED PROVABLE DATA POSSESSION IN MULTICLOUD STORAGE

AUTHOR: Huaqun Wang (2015)

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie- Hellman) problem. Besides of the elimination of certificate management, our ID-DPDP protocol has also flexibility and high efficiency. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

Advantages -- The proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization. It has also flexibility, high efficiency and secure.

Disadvantages -- The complicated certificate management is eliminated.

PUBLIC INTEGRITY AUDITING FOR SHARED DYNAMIC CLOUD DATA WITH GROUP USER REVOCATION

AUTHOR**:** Tao Jiang, Xiaofeng Chen, and Jianfeng Ma (2015)

The advent of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problem of secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. This paper, provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature and figure out the collusion attack in the exiting scheme. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource cipher text

database to remote cloud and support secure group users revocation to shared dynamic data. We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users.

Advantages -- It supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, count ability and traceability of secure group user revocation.

Disadvantages -- The unrevoked members still do not need to update their keys at each revocation.

AN EFFICIENT AND SECURE DYNAMIC AUDITING PROTOCOL FOR DATA STORAGE IN CLOUD COMPUTING

AUTHOR: Kan Yang and XiaohuaJia (2013)

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and thus cannot be applied to the auditing service since the data in the cloud can be dynamically updated. In this paper, an auditing framework for cloud storage systems is designed and an efficient and privacy-preserving auditing protocol is proposed. Then, it is extended protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. The multi-cloud batch auditing protocol does not require any additional organizer. The batch auditing protocol can also support the batch auditing for multiple owners.

Advantages -- It incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the auditing performance and can be applied to large scale cloud storage systems.

Disadvantages -- It is not supported for batch auditing both multiple owners and multiple clouds, without using any trusted organizer.

III. SYSTEM ANALYIS

EXISTING SYSTEM In public cloud environment, most clients upload their data to PCS and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. The computation overhead of verification by the auditor linearly increases with the size of the verified data set. Here third party public auditing theme for the regenerating-code-based cloud storage.

To solve the regeneration downside of failing authenticators within the absence of knowledge house owners, if these information can't be processed simply in time, the manager will face the loss of economic interest. In order to forestall the case happening, the manager has to delegate the proxy to process its data. In PKI (public key infrastructure), remote data integrity checking protocol will perform the certificate management. When the manager delegates some entities to perform the remote information integrity checking, Can it will incur respectable overheads since the voucher will check the certificate once it checks the Remote data integrity.

DISADVANTAGE OF EXISTING SYSTEM -- In open condition, most customers transfer their information to PCS and check their remote information's trustworthiness by Internet.

At the point when the customer is an individual supervisor, some useful issues will happen. The calculation overhead of check by the reviewer straightly increments with the span of the confirmed

informational collection. Here outsider open reviewing plan for the recovering code-based capacity.

To take care of the recovery issue of fizzled authenticators without information proprietors, if these information can't be prepared in the nick of time, the supervisor will confront the loss of monetary intrigue. In request to keep the case happening, the supervisor needs to appoint the intermediary to process its information. In PKI (open key framework), remote information uprightness checking convention will play out the declaration administration.

When the chief delegates a few substances to play out the remote information honesty checking, it will acquire extensive overheads since the verifier will check the authentication when it checks the remote information uprightness.

PROPOSED SYSTEM -- An efficient distributed scheme with data in the cloud is been made. Here we have a tendency to area unit mistreatment the erasure code technique for distribute the info to cloud locations and access the info from cloud. User can register and login into their account. Provided Associate in nursing choice to store, share and access the data from cloud storage. Here we have a tendency to area unit mistreatment the double ensured theme for storing knowledge into the cloud. First is your data or file splited into multiple parts and it will store into different cloud server locations. Each and each file generates the key-code for auditing. Then second is each and every splited file will encrypt before store into different locations. The shared users will edit the go into the cloud with file owner's permission. That file eligible of own public auditing. Search and transfer the files, at the time of download user should use the security key. As an authentication success it will be decrypt and combine to get the original data from cloud. Moreover, we have a tendency to style a completely unique public verifiable appraiser, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our theme will utterly unleash knowledge house owners from on-line burden. In addition, we have a tendency to randomize the code coefficients with a pseudorandom operate to preserve knowledge privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based cloud storage.

ADVANTAGES OF PROPOSED SYSTEM -- Compared to a lot of its predecessors, which only provide binary results about the storage state across the cloud servers, the challenge-response protocol in our work more provides the localization of data error. Unlike most previous works used for guaranteeing remote information integrity, the new theme supports secure and economical dynamic operations on information blocks, including: update, delete and append. Extensive protection and act analysis demonstrate that the projected theme is very economical and resilient beside Byzantine failure, malicious information modification attack, and even server colluding attacks.

III. SYSTEMREQUIREMENTS

4.1.1 SOFTWARE REQUIREMENTS

1) Operating System: Windows XP or Higher
2) Languages used: Java (JSP, Servlet), HTML
3) Tools:JDK 1.7, Net Beans 7.0.1, SQLyog
4) Backend :My SQL

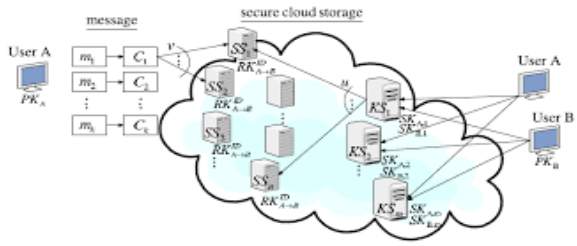
4.2.2 HARDWARE REQUIREMENTS

1) Processor:Pentium Dual Core 2.3GHz
2) Hard Disk: 250 GB or Higher

3) Ram: 1 GB (Min)

ALGORITHM USED

Cloud Secure Erasure -- A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.



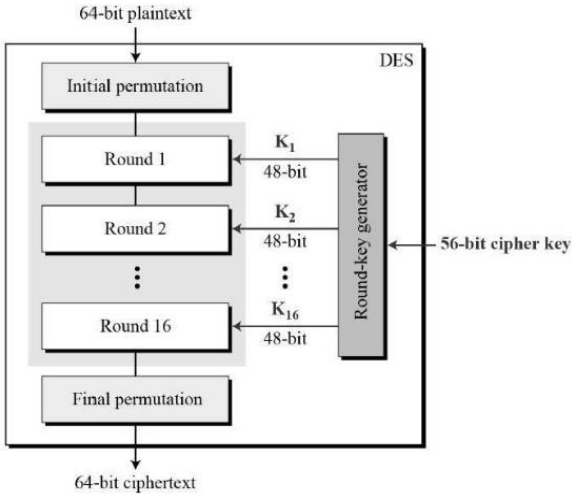
MD5 – The **MD5 message-digest algorithm** is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

A way to take a message of an arbitrary length, and create a 128-bit "fingerprint" or "message digest" of the message. MD5 is a way to verify data integrity. On these forums, it comes up fairly often in discussions about storing user passwords and other sensitive data.

```
$secret_password=md5("password");
if (md5($_POST['password']) == $secret_password)
 {
 echo "Correct password";
 }
else
{
 echo "Incorrect password";
}
```

Simple enough. However, the password is being sent clear text in $_POST['password']. Which brings us to another thing to protect against - the clear text transmission. Thankfully, there is an open source (GPL'd) javascript MD5 implementation available online which can be found here.

DES -- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration.



AES -- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

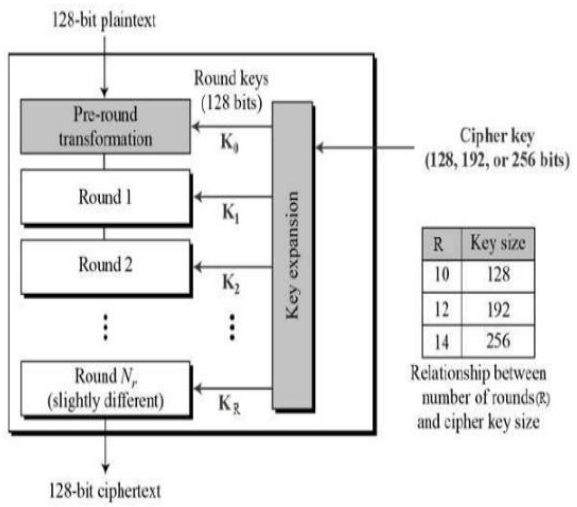
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

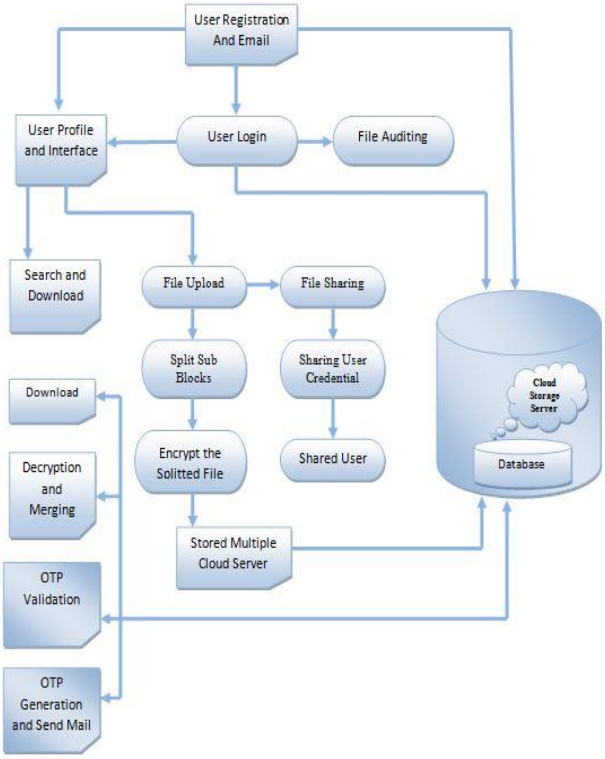
- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES -- AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix – Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.



IV. SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATION

MODULES DESCRIPTION

- User Plug in
- Uploading File
- Secret Key Formation

- File Allocation Process
- File analyzing
- File Loading process
- Alert Mail

User plug in -- In our Secure System we've a user friendly program to move with our System. Every Act dual role as a data owner and data consumer while uploading file they are the owner of that file if they search other's file than they are the consumer. Users can create the account them self for that we have new pages, in that page we will get the details from the user and we generate the account for the user's. We have authentication system; we have a tendency to solely permit licensed users to access our System. In our System we providing the easy file searching user's don't want to keep remember all uploaded file's exact name, for that we have given the keywords while uploading the files it will help to search the file easily.

Uploading File – Storing information over storage servers a method to supply information lustiness is to copy a message specified every storage server stores a message. Another way is to code a message of k symbols into a code word of n symbols by erasure writing. To store a message, every of its code word symbols is hold on in a very completely different storage server. A storage server corresponds to an erasure error of the code word symbol. As long because the variety of servers is underneath the tolerance threshold of the erasure code, the message is recovered from the code word symbols hold on within the offered storage servers by the decoding process.

Secret Key Formation -- Firstly the key are going to be generated because the initial step whereas uploading the file, each that is uploaded, can have distinctive secret key. This key are going to be taken as Associate in Nursing identification of each file. The secret key that we have a tendency to are mistreatment could be a 3 digit range we are going to create it use for each uploading and downloading. If the user want download some file and if he gives the download request the secret key of that file will be sent to the file owner of the file maybe he can share it.

File Allocation Process ---- In our application we can share a file to a registered user by providing basic credentials, with the sharing option it is necessary to provide authority to the shared user whether to view or edit the file. A user can view the shared file within the application without downloading it and the same is possible with the edit option.

File Analyzing -- Auditing is the process of checking the file whether the original contents of the file is changed. This module provides the file owner auditing, this we achieve by generating tokens. The tokens are generated with the ASCII values of the characters in the file and these characters are stored in the DB while uploading the file. If a shared user edit's the file and saves it, again a new token will be generated and stored in the DB. If the initial token and the current token aren't same then a notification will be sent to the file owner.

File Loading Process -- File downloading method is to induce the corresponding secret key to the corresponding file to the user mail id and so rewrite the file knowledge. The file downloading method re-encryption key to storage servers such storage servers perform the re-encryption Operation. The length of forwarded message and therefore the computation of re-encryption is taken care of by storage servers. Proxy re-encryption Schemes considerably scale back the overhead of the info Forwarding operate during a secure storage system.

Alert Mail -- The uploading and downloading method of the user is 1st get the key within the

corresponding user email id and so apply the key to encrypted information to send the server storage and decrypts it by victimization his secret key to transfer the corresponding record within the server storage system's the key conversion victimization the Share Key Gen (SKA, t, m). This formula shares the key SKA of a user to a group of key servers.

VI. CONCLUSION

A protection saving open examining framework for information stockpiling security in processing. We use the homomorphism straight authenticator and arbitrary concealing to ensure that the TPA would not take in any information about the information content put away on the server amid the effective inspecting process, which not just wipes out the weight of client from the dreary and perhaps costly examining assignment, yet in addition reduces the clients' dread of their outsourced information spillage. Considering TPA could at the same time alter varied review sessions from varied shoppers for his or her outsourced data records, we tend to in addition expand our security protective open examining convention into a multiuser setting, where the TPA can play out numerous evaluating undertakings in a bunch way for better effectiveness.

VII. FUTURE ENHANCEMENT

We additionally expand our protection safeguarding open evaluating convention into a multi-client setting, where the TPA can play out different examining errands in a cluster way for better productivity. In imminent we will enhancing the execution.

In this framework we utilized just content records, In future we will incorporate the picture, sound, video documents. In our framework the OTP sent to proprietor mail id, coming up the customer will get the OTP on portable by utilizing the versatile number.

VIII. REFERENCES

[1]. J. Yu, K. Ren, C. Wang, et al, "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2015.

[2]. Q. Wang, C. Wang, K. Ren, et al, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[3]. C. Wang, Q. Wang, K. Ren, et al, "Privacy-preserving public auditing for data storage security in cloud computing," Proceedings of IEEE INFOCOM, pp. 1-9, 2010.

[4]. B. Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2014.

[5]. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," Proceedings of IEEE INFOCOM, pp. 2904- 2912, 2013.

[6]. B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol.8, no.1, pp. 92-106, 2015.

[7]. H. Wang, and Y. Zhang, "On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multi cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol.25, no.1, pp. 264-267, 2014.

[8]. H. Wang, "Identity-based distributed provable data possession in multi cloud storage," IEEE Transactions on Services Computing, vol.8, no.2, pp.328-340, 2015.

[9]. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with

group user revocation," IEEE Transactions on Computers, vol.65, no.8, pp.2363-2373, 2016.

[10]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

Cite this article as :

Deepika. N, Durga. P, Gayathri. N, Murugesan. M, "Proficient Justification of Data Accuracy for Cloud Storage Using Dual Protection", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 2, pp. 287-299, March-April 2019. Available at doi : https://doi.org/10.32628/IJSRST196250
Journal URL : http://ijsrst.com/IJSRST196250