User Level Runtime Security Auditing for the Cloud Using Aes

Ms. Ramya[1], Nikhil Chopra[2], Abhimanyu Wadhwa[3], Ritwick Bhaduri[4]

[1] Assistant professor, [2,3,4] UG scholar

DEPARTMENT OF COMPUTER SCIENCE
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

Email: ramyak2@srmist.edu.in[1], nikhilchopra6002@gmail.com[2]
abhimanyu18n@gmail.com[3], ritwickbhaduri7@gmail.com[4]

***Abstract*—With the demand of human increases and evolving of technology increasing rapidly, there is lot of data which is there to store on internet and with the help of Cloud Computing which delivers processing power and application to storage. No need to own large infrastructure or large data centers which limits the cost and complexity of owning and maintenance the large infrastructure. It is like pay for what they use. Through Natural language processing, Artificial Intelligence and standard office application cloud computing covers range of options like processing power, networking and storage.We suggested a framework which is privacy-preserving framework that allows for public reviews of cloud-based shared data.From the studies found, cloud computing evolved towards upper curve of graph. An effective public auditing protocol need to be developed which overcomes the auditing schemes. It is created to ensure that cloud data was accurate using Third Party Administrator. During review process, it ensures that no data material is leaked to third parties. The user or owner is in control for dividing files into blocks and generating MD-5 botch value using various algorithm. The encrypted files or blocks are stored in cloud server. Hash values are then concatenated and AES signature is generated for the file.**

***Keywords* —Cloud computing, AES, MD5**

II. INTRODUCTION

In cloud to do public auditing on data shared we put forward a privacy - preserving mechanism. Also, we make use of ring signs to gauge metadata verification to audit accuracy of shared data. Instead of checking them one by one our system is doing multiple auditing tasks at the same time.In shared data, the signer specification on each block is kept hidden from external parties and there is no need to retrieve the whole file for the verification of the shared data.

As we are doing the privacy-preserving public auditing task for the data which is shared in cloud, there is method called ring signatures which we build for homomorphism authenticators which further help it to secure the private data and by not retrieving the whole file or data but still, we cannot check each block belong to which signer. Therefore, to overcome that problem we are keeping the mechanism in batch auditing to verify multiple auditing tasks.

For further problems, there are still few studies which will continue such as the trace ability, that is for the verification of identity of signer there will be a manager which will control all the metadata and helps to reveal all the confidential data in certain conditions.

The Algorithm used here is AES which is associate degree. By using AES, we can perform various operations such as exchanging of various input by distinct outputs and also jumble them around. It is basically first substituting the network then permutate it.

AES does work on bytes rather than performing on bits. Therefore, for 128 bits it can be read as 16 bytes. Its further result in 4x4 matrix which is organized in systematic order of 16 bytes square.

III. RELATED WORKS

Cloud is just a metaphor which works in such a way that make the large server – farm infrastructure of data center over internet via cloud which saves lots of money and space. That's why large MNC's and institutions are sliding towards putting their large data into cloud because it is highly secured and there are lot of advantages which no one can ignore. When accessing through a hard drive we know it took lot of time and has a chance of corruption that may leads to loss of important data. Therefore, via cloud using internet with one click you can use the data you need anywhere and at any time.

Sherman S, Cong Wang Qian Wang made a privacy preserving auditing system by making MAC random masking and constancy dynamic authenticator. Constancy dynamic authenticator and random masking ensures that there will be no leakage of data and third party cannot have any knowledge of data stored in cloud. It is an efficient process and one can be relaxed from their data leakage. The main problem is individual auditing task is really hectic and not possible for large storage. The public key-based homomorphism executes reviewing without requiring a local copy of the results, lowering communication and measurement costs.

Y. Prasanna and Ramesh created an efficient multi keyword search by using Ranking method and symmetric key encryption which is highly secured and based on a password-protected database that is held on a remote server model that protects database user's privacy. Instead of using for report encryption, use social encryption, they used symmetric-key encryption to improve the scheme's performance. The ranking approach has proven to be effective in returning highly relevant information. The problem is this approach has high computing and communication costs because each multiple secret sharing encryption techniques have been found on both the server and client sides for such a keyword in a query, and retrieving all containing information the queried parameter adds to web traffic.

Boyangwaang, Baochun lii and Hui lii created the TPA, that can easily examine the mutual data's honesty, and it also can't say who's each block's recipient, protecting users' ethnicity security. They used to generate the circular keysidentification required details to review shared data veracity. The problem is since the signer's characteristics on mutual data can mean there is a specific handler in a community or you can say specific a more important target than others is to create a block of shared data, it stands important towards protect identityprivacy from the TPA.

Boyang wang and Baochun li created public auditing using resigned techniques that enable the moderately database to use proposed multi examples to re-sign columns signed by the revoked user. when a user in the community is revoked. During user revocation, the community will save a large amount of computing and communication capital. The problem is the confidentiality of the login credentials of current users can then be used to verify the entirety of the data and this revoked handler may no longer able to access then change shared data.

Bo chen, and Reza curtmola created an scheme for distributed databases based on network coding that depend on unauthenticated servers that is both secure and effective. If data is stolen, reloaded, or damaged, the scheme is used to maintain data integrity. The scheme is a low-cost solution for mutuallyconsumers and attendants. The problematic is thatcipher is not organized, the input is non inserted as a portion of the production that has been preserved and slightportions of the folder cannot be repossessed without restructuring the completefolder. They use hierarchical codes to support data access to sub-files. Network-coding for storage is only practical in networks where data repair is much more common than reading.

Dan Boneh, Xavier Boyen and HovavShacham created signatures using RSA algorithm that are around the same size as a generic RSA signature and provide the same level of protection. The squad sign is erected on the

Strong DH presumption and the Decision Linear, a new bilinear group statement. The problem is the signature generation does not necessitate any pairing computations, whereas verification only necessitates a single pairing.

BoyaangWanng and Sherrman S. Chhow and Miing lii assumed using PDP as well as signature that the best way to achieve privacy while packing data in cloud while preserving data honesty that is openly verifiable. The use of a security mediator make private part of the structure is isolated from the demonstrable data and security mechanism. They reduce the intermediary's computation and bandwidth requirements while also reducing the degree of confidence held in it in terms of data and identity privacy. Thechallenge is that the roles of current members on shared data may show that an user or a certain block in unlimited memory is a more worthwhile priority than others, it remains important to protect uniquenessconcealment from the TPA. The information is private to the community and should not be shared with someone else.

A complex audit service for untrusted and outsourced storages is being developed using key generation algorithm and tag generation algorithm. It was also introduced an effective method for performing periodic sampling audits to help TPAs and storage service providers improve their performance and which reduces the cost of computing and communication. The problem is this auditing process is ineffective.

IV. EXISTING SYSTEM

In the Existing system there are substantial privacy problems which are there when we share data which leads to outflow all the confidential data to public. Previously what it does is retrieving all the data for data accuracy from the cloud , and then verify the completeness, accuracy and consistency of signatures.

The main problems faced in existing system are firstly as users who are loading their confidential data into the cloud cannot physically own the storage, thus the old-style cryptographic style for the security of data cannot be used as it leads to the loss of confidential data and also not highly encrypted. Using the current system, we also cannot perform the multiple review at the same time. The process is also slow therefore to identify the user it takes lot of time which is very hectic. One can led to loss his entire data due no privacy. As there is no auditing in the system various new vulnerabilities are caused towards user data privacy.

A.Modificationto the existing systems

1. By the use of privacy – protection mechanism to store the shared data in cloud, a user can easily review the desired data without retrieving all the data by making ring signatures.

2. By making the batch auditing of data, it improves the productivity of reviewing multiple tasks.

3. Traceability: By making managers who can reveal the confidential data of the user in certain condition.

4. To send the important and confidential data over the cloud or web, we can use SMTP which is Simple Mail Transfer Protocol. Using this protocol, we can directly send electronic message.

5. Pop3 and Imap are the incoming mail servers which are there to set mail of account’s server which is different from SMTP server.

V. SYSTEM SPECIFICATION

Software Requirements:

- Programming Language – Java (JDK 1.7)
- OS – Windows 7 32-bit
- Server - MySQL Server

- IDE - NetBeans IDE 7.1.2

Hardware Requirements:

- RAM - 1 GB
- Hard Disk - 80 GB
- Processor - More than 2 GHz
- Card - Data Card

VI. PROPOSED SYSTEM

A. Explanation

In the proposed system, we admittance shared data inside the cloud through a privacy-protective public reviewing mechanism. In order to construct homomorphism authenticators, we use ring keys to ensure that a common verifier cannot be established. while he is reviewing shared data integrity without actually fetching the entire data, in this way, we would not be able to distinguish between signers of each block.

We cover our device to support setreviewing in order to improve the worth of verifying numerousresponsibilities of reviewing. For our future work, we will go through two intriguing problems. The first one is called traceability, which is how the collectionsupervisor can disclose the uniquenessof signer in some special cases through verification or authentication metadata.

We have also briefly described SMTP which is the acronym for 'Simple Mail Transfer Protocol. It could be used for web causation e-mail. SMTP has been used by the email customer to transmit a letter to the mail server.SMTP is also used by the mail server to relay that message to a proper mail server for receiving the content. It is nothing but a set of commands which direct and authorize the transfer of an electronic message. SMTP server should always be set to the user's native net after configuring the e-mail program settings. The incoming mail sever, which is IMAP or POP3 is supposed to be set to the user's mail account, and it can differ from the SMTP server.

B. Advantages of the Proposed System:

- Requests can be sent to the auditor by the users.
- It provides high security for sharing of files.
- Users can be deleted by the admin as per requirements.
- Multiple compliance procedures can be accomplished at the very same time.
- Through this system, Verification reliability can be increased for a variety of reviewing activities.

C.System Architecture:

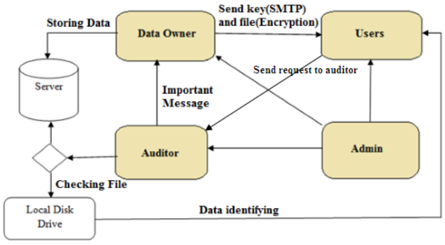


Figure X: System Architecture

D. Algorithm:

Advanced Encryption Standard (AES):

The AES algorithm is used for encrypting and protecting important yet non-classified knowledge by US federal agencies, and may become the sole legal authentication protocol used throughout the corporate companies to finish economic activities. After all, authentication for US diplomatic and other restricted interactions is managed by a specific factor that we are not aware of such process.

And in initial part of 1997, the NSIT took the first steps to find a stronger and more robust substitute only for DES which is Data Encryption system. This necessitated an encoding scheme, which was resolved using decoding of 128-bit block. These were provided wealth to be used anywhere around the globe and was configured to include appropriate consumer protection for the next two to three decades. It was not complex to realize the method in software and hardware, and in many other controlled situations like smart card. It also provided a strong defensive mechanism vs a variety of hacker attacks.

The process was kept open to public feedback and comments, since they thought that it was the best method to analyze the designs.

Among the most recent sections throughout the evolution of encryption is AES. After it became apparent that no other DES nor even the response to its flaws, Triple-DES might bring encoding into the twenty-first century, the NIST issued a directive to create a new model. AES was chosen over other protocols for a variety of purposes, and it has become one of the most widely used cryptographic protocols. Its presence on the desktop is typical for employees who work mostly in security sector. It also benefits from unrestricted promotion and recognition as a result of its designation as an approved encryption framework in 2001. In May of the subsequent year, this category went into effect. The above section of the study is largely a reimagining study mostly on FIPS 197 model, as it happens to be among the most definitive manuals provided outside of the researchers' own. It includes a few unique instances as well as the author's findings from his review of the norm.

Fifteen candidates were selected by the NIST in 1998 for the AES also was subjected to systematic review by some world statistical organization, which would include the NSA i.e., National security agency.In 1999, NIST selected five algorithms on the basis of this for further in-depth analysis.

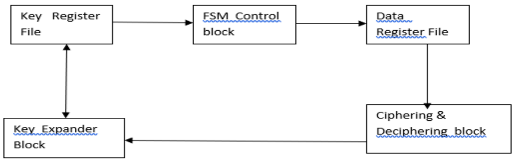
AES uses bilinear pairing boxes to encode symmetric key in a sequence of circles, close as DES. It uses an encryption and block dimensions, as well as replacement as well as sequence boxes. In the following situations, it varies in DES:

- Block dimensions of 128 bits are supported.
- The S-box is used to create the main plan.
- The main is expanded, not the plaintext.
- It doesn't use an Ellamae cypher.
- It's a confusing case.

Decoding rates, code and method initialization time, including attack tolerance were all tested thoroughly from both hardware / software frameworks using the computer languages. The international computational group offered a thorough examination, and now the final result was revealed on 2nd October 2000.

The DES was used until AES was widely adopted, but it was growing highly susceptible to physical attacks. And this is why the NIST declared that perhaps a stronger and much more mature alternative for DES was urgently needed. As a result, AES was adopted as a superior, more recent, and also more sophisticated asymmetric encryption. AES was designed to shield country sensitive data at first. It is commonly seen in defending against even a variety of computer hackers' tactics, like overwhelming strength, since it is simple to incorporate in both operating systems. AES is also used for instance in industrial and anti-services by both individuals and organizations. However, US export restrictions place certain restrictions on semi entities.

E.DIAGRAM



VII. RESULT AND DISCUSSION

The results can be listed below:

1. The entire problem domain cycle was conducted and numerous approaches for solving the problem were extensively examined.

2. The privacy-preserving public auditing mechanismhas been built successfully, all algorithms added in it are working properly and improve the efficacy of verifying multiple tasks of auditing.

3. The Algorithm AES is being successfully used and can perform various operations such as exchanging of various input by distinct outputs and also jumble them around.

4. Finally, the paper was pleased with offering privacy-preserving public auditing mechanism, in order to construct homomorphism authenticators.

VIII.CONCLUSION

We analysed that the existing system for cloud stored data security has unsolved problems like users cannot own the storage, and multiple review cannot be performed on the stored data. But with the mechanism proposed here auditing on the data is possible in parts without fetching the entire data. Also, the system supports batch auditing in order to improve the efficacy of verifying multiple tasks of auditing.

IX. FUTURE WORK

1. Introducing traceability, which is how the clustersupervisor can disclose the uniqueness of the person in some special cases through verification or authentication metadata.
2. Application of the system to all accessible cloud storages.
3. The system can be made much simpler, i.e., less voluminous in design.
4. Introduction of more authenticity for public trust and usage of the system.
5. Collaborations with Cloud Storage industries

X. REFERENCES

1. B. Wang, B. Li, and H. Li, “Certificate less Public Auditing for Data Integrity in the Cloud,” Proc. IEEE Conf. Comm. and Network Security (CNS’13), pp. 276-284, 2013.
2. C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.
3. B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” Proc. IEEE INFOCOM, pp. 2904-2912, 2013.
4. Y. Miao, X. Liu, K. Choo, et al.,“Privacy-Preserving Attribute-

5. Based Keyword Search in Shared Multi-owner Setting”, IEEE TDSC, DOI.10.1109/TDSC.2019.28976752019.
6. R. Chen, Y. Mu, G. Yang, et al., “Dual-server public-key encryption with
7. keyword search for secure cloud storage”, IEEE TIFS, vol. 11, no. 4, pp. 789-798, 2015.
8. M. Armbrust, , A, . Fox, , R, . Griffith, , A, et al., "A view of cloud computing", *Commun. ACM*, vol. 53, no. 4, pp. 50-58, 2010.
9. J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication", *Proc. IEEE Conf. Commun. Netw. Secur.*, pp. 145-153, 2013.
10. S. Halevi, D. Harnik, B. Pinkas and A. Shulman-Peleg, "Proofs of ownership in remote storage systems", *Proc. 18th ACM Conf. Comput. Commun. Secur.*, pp. 491-500, 2011.
11. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, et al., "Provable data possession at untrusted storages", *Proc. 14th ACM Conf. Comput. Commun. Secur.*, pp. 598-609, 2007.
12. G. Ateniese, , R, . Burns, , R, . Curtmola, , J, et al., "Remote data checking using provable data possession", *ACM Trans. Inform. Syst. Secur.*, vol. 14, no. 1, pp. 1-34, 2011.
13. G. Ateniese, R. Di Pietro, L. V. Mancini and G. Tsudik, "Scalable and efficient provable data possession", *Proc. 4th Int. Conf. Secur. Privacy Commun. Netow.*, pp. 1-10, 2008.
14. C. Erway, A. Küpçü, C. Papamanthou and R. Tamassia, "Dynamic provable data possession", *Proc. 16th ACM Conf. Comput. Commun. Secur.*, pp. 213-222, 2009.
15. Y. Zhu, H. Hu, G.-J. Ahn and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage", *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
16. Q. Wang, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", *Proc. Comput. Secur.*, pp. 355-370, 2009.
17. E. Stefanov, M. van Dijk, A. Juels and A. Oprea, "Iris: A scalable cloud file system with efficient integrity checks", *Proc. 28th Annu. Comput. Secur. Appl. Conf.*, pp. 229-238, 2012.
18. J. Li, X. Tan, X. Chen and D. Wong, "An efficient proof of retrievability with public auditing in cloud computing", *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, pp. 93-98, 2013.
19. W. K. Ng, Y. Wen and H. Zhu, "Private data deduplication protocols in cloud storage", *Proc. 27th Annu. ACM Symp. Appl. Comput.*, pp. 441-446, 2012.