Secure Ring Signature based privacy preserving of Public Auditing mechanism for outsourced data in cloud computing paradigm

D Srivaishnavi¹, T Arjun², K Dhyaneshwaran² and R Deepak²
¹Sri Krishna College of Engineering and Technology, Assistant professor, Department of CSE, Coimbatore, India
²Sri Krishna College of Engineering and Technology, UG student, Department of CSE, Coimbatore, India
srivaishnavid@skcet.ac.in

Abstract. Cloud computing offers a high scalable environment for data outsourcing in the cloud. This allows a user to access all the cloud applications of any complexity, without thinking about the limitations of the local system infrastructure. It also provide medium to share the data among others. However originality and authenticity of data that is stored in cloud is an open challenge as it has large provision for data lose and date correction. In order to prevent the outsourced against various challenges, many tradition data auditing mechanism on employing third party auditor has been provided in the literatures with computation and communication capabilities. A portable data management system to will be able to perform auditing process, so that we can ensure the accuracy of the data which is stored on a unreliable third party server. This process is done without even, retrieving all the data. Despite of various advantage of public auditing, preserving the identity privacy from third party auditor has become vital task for the current research. In this paper, we have proposed a reliable and secure ring signature for preserving the privacy of data that is outsourced and shared, using public auditing in the computing paradigm. In this work, ring signature is exploited to privacy preserving of the data auditing of common outsourced data. Further the idea of ring-signatures has to be used to build the authenticator on each block of the data that is outsourced, while keeping maintaining the authenticity of the shared-data to be audited. Finally this model can support multi auditing task simultaneously. Experimental analysis on the proposed system proves that it is more secure and highly efficient against data based attacks. Evaluation the performance of the proposed model has been validated that it outperforms state of arts approaches on computation cost and time.

Keywords: Data Integrity, Privacy preserving, Cloud Computing, Public Auditing, Outsourced Data

1. Introduction

Cloud-Computing is emerging as the next-gen design for data based services towards sharing of data with many user. Many strategies have been proposed for auditing purposes of cloud-data health with focuses on the supporting the changing data, auditing the public data integrity, less transaction and computing cost on data auditing, and less overhead storage to ensure users trust in the data integrity of their data that is shared on cloud. To conclude, the cloud data accuracy is compromised due to the
wide variety of inbound and outbound threats for the data in cloud [1]. Without the offline copy of the
data, properly ensuring the quality of data in cloud that is extracted becomes a major security problem for data that is stored in a Cloud Server [2].

Viewing in the point of view of privacy protection of data users, who has the rights on the data and relying on the TPA mainly for ensuring security of their data that is stored in cloud, data-owner does not accept this testing procedure to introduce many risks of unknown data leaks in the security of the data. The signature signing process based on public research on homomorphism mandated along random mask technique for supporting data confidentiality while public research, as well as the hash-table with index for supporting of the full performance on the cloud shared-data. In addition, we continue to expand our approach to supporting belt research, that can research many of the shared-data in cloud simultaneously within one auditing work [3]. Powerful operation suggests adding, removing or re-activating one block in the shared-data in cloud [4].

The reminder of this paper is organized as follows. In Section 2 we have discussed related works for this system, and in Section 3 we give a brief introduction to the proposed system model and describes the system in a detailed manner. Section 4 examines and evaluates results using various criteria. Section 5 concludes with a recommendation for further study.

2. Related works

In this current section, the process of maintaining confidentiality by public auditing in social research programs that allows clients to store data in the cloud and create privacy across the entire data block is discussed in detail as follows

2.1. Confidentiality-preserving public auditing data

In this paradigm, the time-specific details of each document in the collection of indices, such as in traditional retrieval systems for transparent writing have been analyzed. The confidentiality of orders ordered by rank is considered to be the framework for the integration of appropriate measurement methods and cryptographic strategies in providing efficient and accurate search capabilities to protect order documents by answering the question [5].

2.2. Enabling secure and efficient public auditing over outsourced cloud data

In this paradigm, confidential data in the cloud must be securely encrypted using algorithms before exporting using encryption methodologies that are searchable which allows data-users to safely search the data that is encrypted with keywords. In the model that is proposed, we use AES algorithm for encryption. In this limited search it significantly improves system utilization by enabling rating results unlike sending results are unnoticed and again ensuring the accuracy of retrieving the file in point scores associated with building a secure searchable index [6].

3. Proposed model

In this section, firstly we introduce the basics followed by the architecture of the proposed model that is described in detail on specific aspects.

3.1. Notations and other Preliminaries

F- data that is outsourced or stored in cloud, containing blocks m1, m2, 3... mn

Mac-key-Message authentication code

H- Mapping of hash functions to some group
3.2. Bilinear Map Pairing

A pairing is a bilinear map defined over groups. Let’s consider \( G_1 \) and \( G_2 \) as sub-groups of the same prime order \( q \). Multiplicative group of the order \( q \) is represented by \( G_T \). Both \( G_1 \) and \( G_2 \) are generated by points \( P \) and \( Q \).

Representation of Bilinear Map is \( G_1 \times G_2 \rightarrow G_T \) after satisfying the following properties,

- **Non-Degeneracy**: Let the generators for \( G_1 \) and \( G_2 \) be \( P \) and \( Q \) respectively in which neither \( G_1 \) nor \( G_2 \) contains only the point at infinity.
- **Computability**: Verification of the group.

3.3. System Model

In this section, each cloud business is described in detail with its operating process carried out to achieve a specific goal. In the community, there are two categories of users: the initial user and the total number of users. There are two categories of members, one is original users and other is group users. According to the access-control rules, team members are given permission to access and change shared user-generated data. The cloud server stores both shared data and its authentication information (e.g. signature).

![System model of proposed mechanism](image)

**Figure 1.** System model of proposed mechanism

On behalf of the team members, a third-party investigator may check the accuracy of shared information on the cloud server. Figure 1 represents a system model for the proposed method of assessing with dynamic communities, the credibility of shared data in the cloud [7].

3.4. Data Auditing

When the data owner decides to start verification, for the authenticity of the data that is shared, the data-user submits an auditing request to third party auditor(TPA). Upon receipt of an audit request, third party auditor generates an audit message on cloud-server, after which he receives proof for the shared-data that needs to be audited from the cloud service provider. The third party auditor(TPA) subsequently starts verifying the accuracy of the data auditing evidence [8]. At last, third party auditor will send an auditing report for the requested file, to the user as a result from the verification result.

3.4.1. Index Tree Construction

Initially, index tree that isn’t encrypted (T) is created on \( F \) with index tree build function. Next the data-owner(Do) generates two different vectors \( D_u \) and \( D_{u|} \) index vector with respect to to the confidential vector \( S \) from the unique words extracted from \( C \).

Index Tree build function is given by

\[
T = \text{buildindextree}(F)
\]

\[
\text{buildindextree}() 
\]

for all document in \( F \)
do.
    construct sub set u for document f
    insert u to current set
  end for
while ( no of subset > current set )
  do
    if ( no of keywords in current set is even )
      then
        Increase new set to the store the hashed data
      End if
    End for
  End while

3.4.2. Ring Signatures
The ring signature is generated for dynamic forming group by the owner to access of the classes of data files. Ring signature takes the Master MSK abbreviated as the master secret key and public keys of the data user PK, to generate the ring signature Rs. It is processed using a hash function to generate a hash value. The following conditions should be met by a signature scheme that verifies homomorphism authentication using signatures. [9]

- Blockless verification
  The authenticator can verify the validity of the data stored on the cloud server with a single block, which is a linear combination of all data blocks, using blockless verification method. The authenticator assumes all data blocks are right if the combined block is correct. As a result, there is no necessity for the authenticator to download maximum of the blocks in order to verify the data's integrity [10].

4. Experimental Results
In this result obtained from experiment section, we analyse the privacy preserving of the proposed public auditing method against the state of art approaches on various data size. Further, for various security results it has been computed and defined in terms of performance charts and tables and measures like memory utilization on computation cost and time. The system's dependability is determined by the use of proxy server technology in data sharing systems. It will make delegating access rights to other participants much easier for the data owner.

![Figure 2](image_url)

**Figure 2.** Evaluation of memory use on proposed and current models for different file sizes

The output performance of the proposed model and current models to various files is described and summarised in figure 2 and table 1. Memory utilization time is increased due to utilization of the privacy preserving on basis on block which stores the data of any user.
Table 1. Evaluating the performance of the Security Model

| Technique                | No. of File or File Size | Time Take in ms |
|--------------------------|--------------------------|-----------------|
| Merkle Hash Tree-Existing| 5                        | 36000           |
| Ring Signature – Proposed| 5                        | 24000           |

The proposed model has high memory utilization as it enables the thresholding model for hiding the index and data. If the data owner wants to change an existing record, the user will create a new index for it so that a third party auditor won’t be able to access it in the future.

5. Conclusion
We proposed a concept and implemented a ring signature-based privacy-preserving auditing scheme in a multi-authority setting to create a stable and a scalable data sharing model. The proposed model illustrates the system’s effectiveness in terms of key generation, encryption, and decryption for different file sizes and group member creation. On sharing multi classes of files to a group of users, the importance of ring signature and aggregate key use has been explained in detail. This model has been shown to be effective across a wide range of data groups. The use of storage and time has been shown in the experimental research.

References

[1] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[2] M. Li, S. Yu, N. Cao, and W. Lou, Authorized private keyword search over encrypted personal health records in cloud computing, in ICDCS ’11, Jun. 2011.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in Proc. of ESORICS’09, Saint Malo, France, Sep. 2009.

[4] Halderai, A. Ramu, and S. Murugan, Social Aware Cognitive Radio Networks, Social Network Analytics for Contemporary Business Organizations, pp. 188–202. doi:10.4018/978-1-5225-5097-6.ch010

[5] R. Arulmurugan and H. Anandakumar, Region-based seed point cell segmentation and detection for biomedical image analysis, International Journal of Biomedical Engineering and Technology, vol. 27, no. 4, p. 273, 2018K. Liang, Q. Huang, R. Schlegel, D. S. Wong, C. Tang, A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release, In Proc. Information Security Practice and Experience , pp. 132-146, Springer Berlin Heidelberg, 2013.

[6] J. Byun, D. Lee, On a security model of conjunctive keyword search over encrypted relational database, Journal of Systems and Software, vol. 84, no. 8, pp. 1364-1372, 2011.

[7] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, Efficient Unidirectional Proxy Re-Encryption, in Progress in Cryptology - AFRICACRYPT 2010, ser. LNCS, vol. 6055. Springer, 2010, pp. 316–332.

[8] C. Hu, P. Liu, An enhanced searchable public key encryption scheme with a designated tester and its extensions, Journal of Computers, vol. 7, no. 3, pp. 716-723, 2012.

[9] D. Boneh and D. M. Freeman, Homomorphic Signatures for Polynomial Functions, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2011, pp. 149–168.