ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 10, Issue 5, November 2020

Integrity Monitoring with ECMRSA Algorithm for Cloud Data Outsourcing

D V Thang, N D Pham
School of Computer Engineering, Vietnam

Abstract: ***With its on-demand technology, cloud computing has advanced to allow vast volumes of data to be interchanged via cloud services. Scalable cloud services that store confidential data on cloud storage servers are therefore critical to the complex management of a number of problem fields: security, privacy, data sharing and cloud server integrity. In addition, in this expanded environment, validity and control of access to data should be retained. One of the core principles for cloud encryption is abe. An interest in this research is the auditing of data or integrity tests for secure cloud storage. The data audit approach allows an auditor to verify the consistency of the data files and submit the data owner's verification report, without understanding the files. This paper offers an RSA modified elliptic curve (ECMRSA) and an algorithm modified to md5 for the purpose of verifying the integrity of cloud data, to upload the encrypted data files of data users or proprietors to the cloud data server and send a request for a third-party audit to the auditor. On behalf of data holders, a third-party auditor (TPA) is called by the data server to ensure the file is credible. The auditor sends the audit report to the owner following maintenance of the data file accuracy. A public key coding scheme with homomorphic algorithms that produces a digital file signature or hash values for coded files is included in the proposed audit algorithm.***

Keywords: **Cloud Computing, Monitoring, Data sharing, Security, ABE.**

I. INTRODUCTION

Amongst all emerging technologies that the business community deals with, Cloud Computing in the present scenario stands apart. Although it is advantageous to have cloud computing, security of the data stored is of prime concern. It is not easy to manage and maintain large amount of data on local systems and hence storing the data on cloud relieves the burden of data owners. The major advantage of cloud storage is that, it can be updated at any time and stored form anywhere or itcan be said that it is location independent storage [3]. According to the Cloud Security Alliance (CSA), amongst the most prominent seven security challenges related to cloud computing, leakage and loss of stored data is the second most dealt with threat [2].

Once the data or database is shifted from local systems to the cloud, CSP takes the charge and starts managing data [4]. The initial data owner does not have control over the data at this stage, which poses a major security concern. Primary concern in database outsourcing is that once it is outsourced, it becomes prone to harmful attacks. Apart from this the server itself may cause harm to stored data by modifying or deleting it or inserting unnecessary data.

Manuscript received: 25 October 2020
Manuscript received in revised form: 20 November 2020
Manuscript accepted: 07 December 2020
Manuscript Available online: 15 December 2020

Necessary steps that are required to be taken before the data is outsourced can be briefly summarized as follows:

- ***Confidentiality:*** it is of utmost importance that the outsourced data is encrypted, so that it remains safe from unnecessary harmful external or internal attacks.
- ***Integrity:*** Any insertion or deletion of data from unauthorized sources should be avoided and the data owners should be able to protect it from such modifications. Any incomplete or corrupt data should be easily identified by the data owners and they must make sure that they have their data in the most updated version, so that their data remains consistent and accurate.
- ***Availability:*** The data owners should make sure that have access to their data stored in the cloud servers. The data owners may sometimes lose access to their database due to natural disasters, certain attacks known as Denial of service, failure of equipment of the one who provides service.
- ***Access Control:*** Any unauthorized user should not be able to access the data by any means.

Considering Remote Data Integrity Checking (RDIC), conventional technologies of cryptography for checking integrity of the data such as codes of authentication and digital signatures should not be used. It is because of the necessity of original file in the verification process. Downloading the file entirely for verification from cloud is a cumbersome task. At present, integrity checking of data at the servers is primary area amongst researchers across the globe. The objective of this research is to deal with the audit of data integrity checking by an authorized Third Party at the cloud servers. The primary aim of the present work is study all protocols pertaining to data integrity checking related to cloud servers [6-8].

The prominent areas that are dealt with in the present work are as follows:

- Threat and system models for database outsourcing in the cloud.
- Various protocols have been compared on the basis of strategies pertaining to security, prices of computation, overhead data storage in the cloud and costs related to communication
- Challenges in auditing protocol related to data integrity.

The primary goal of this research is:

- Working towards building a data integrity scheme that is attribute-based, so that data users find it easy to upload files and produce secret keys utilizing some attributes.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 10, Issue 5, November 2020

- Also, a Third Party Auditor (TPA) can be specified by the initial data owners who will be able to have a close look on the outsourced data integrity [9].

II. RELATED WORK

An ID based-RDIC (Remote Data Integrity Checking) along with its security model was proposed by Yong Yu in his research [2]. The model also includes security against harmful cloud servers and keeps it safe from external auditing. No information pertaining to the data auditor that is stored is left behind in the DRIC process by the protocol. Amidst the generic group template, the new model was successfully demonstrated to be safe against harmful servers. The model also represents zero knowledge confidentiality for an external auditor. In depth analysis and implementation of the protocol has made it very clear that it is completely safe and can be successfully applied for practical applications.

To accomplish the objective of secure cloud storage, RDIC or Remote Data Integrity Checking is area that should be seriously dealt with. This is also discussed in the research work by Sasikala [5]. It nullifies the need to download complete data from cloud for checking outsourced data integrity. An in-depth analysis of the RDIC protocols has been done in the present work and also its classification has been discussed. For instance, Proof of Ownership (POW), Provable Data Possession (PDP), Proof of Retrievability (POR) and ID based RDIC protocols. A detailed analysis and comparison has also been made between the various RDIC approaches considering auditing mode, method of integrity checking, recovery of data and cryptographic model as their basis. A public auditing scheme that is intended to produce key value and is certificate less is proposed by T Subha and R Swathi [7] in their research improving the security of data stored in the cloud. To keep the private key of the user completely safe, a partial key is generated by the Key Generation Centre (KGC). This private key is then utilized to produce public and private keys which can then be used to check reliability of the data stored in the cloud server. A detailed report is sent to the data users once it has completed checking.

With an objective of reliability in data within an auditing process, blocks are randomly selected and proof is generated by the server. The proof is then verified by the TPA for the cloud server and the user's results are audited. To tackle the primary management challenges, an auditing protocol based on attribute was put forward by Yong Yu [8] in his work. The mathematics involved was reduced to a great extent through this method and hence the analysis could be done in much less time.

A unique approach was proposed by Yannan Li [10] in his work. He proposed a unique identity based auditing approach to tackle the primary management issue while checking data integrity. It was unique in its own way as the identity of the one who uses it could be observed as a set made of attributes that are descriptive in nature. For this unique approach, security and system models were finalized. A solid foundation of the indistinct auditing protocol that is identity based is then presented by us by using biometric for identity purpose. The major advantage of the newer protocol is that of tolerance of errors. It helps in binding a specific identity to private key. If an identity is very close to the specific identity, it helps in the verification of response generated by it. The security issues of the protocol were dealt with considering the discrete logarithm and Diffie-Helman assumption for the security model of selective ID.

It is a well known fact amongst the users that cloud servers cannot be completely relied upon. If any data or server is accidentally damaged, entire database of the data owners gets lost making it a very risky storage media. Whenever such accidents occur, roll back techniques come into play and recovery of data files is the done from the backup servers. The major challenge from the data restored from back up servers is that they are recovered in some previous state. At this point of time it becomes utmost importance to apply data integrity checking for the data so that it gets correctly stored by the cloud servers. Hence, the need of the hour is to develop an integrity mechanism that is efficient but not complex.

III. METHODOLOGY

The audit system at present should work with an objective to design a strong audit protocol that is public and deals with all of its challenges. The proposed protocol has been made in such a way that it will have a close look on the data stored with help of TPA. Also it will not increase the load on cloud servers and its users. It will also make sure that it does not affect TPA while doing its job. At the same time it makes sure that the confidentiality and statistics of data is not overlooked.

The three building blocks of the system that is proposed include: Third Party Auditor, owner of the data and cloud server storage. It is the responsibility of the data owner that their data is properly hashed and concatenation is applied on them. Also they must make sure that their file is divided into blocks, encrypting the data. The block are then stored on the cloud servers in encrypted form. If the validation of data is to be done with the Third-Party Auditor, the stored data is instantly accessed from the cloud servers.

Once the data is received, harsh algorithms for file blocks that are encrypted get generated. An algorithm similar to that utilized by the client is generated. A perfect match proves that the data is maintained in its original state and is not attacked by any external source. An if it does not, and then it is a sign that the data was improperly managed and was attacked. The owner of the data then receives the result. A schematic for the proposed work is presented in figure 1.

Cloud data integrity Auditing was introduced to solve this problem, Amongst others Provable Data Possession (PDP) was of prime importance. It is basically a detection protocol with a probabilistic approach. It randomly selects blocks for integrity checking instead of going through the entire file. When larger files are dealt with, this approach seems to be the most efficient.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 10, Issue 5, November 2020

The approach employed in this research is different from others in the way that attributes based validation o data stored in the cloud s employed. The integrity assessment through this approach is greatly simplified as the data users can now easily use cloud servers to upload files with the use of specific attributes and even designate them. The private key is generated through different attributed ant the performance is easily analyzed.

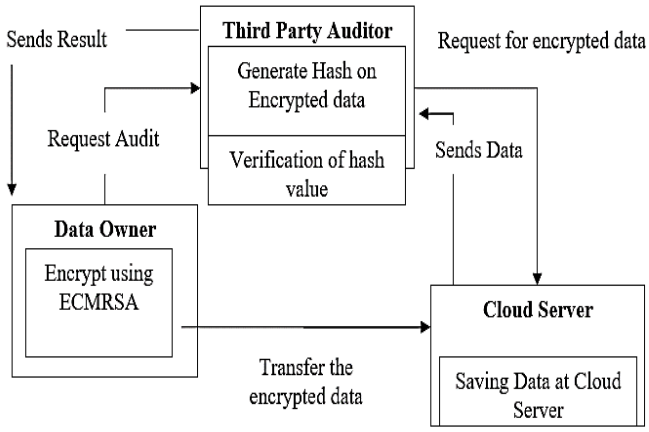

Fig.1. Proposed Architecture-Level-1

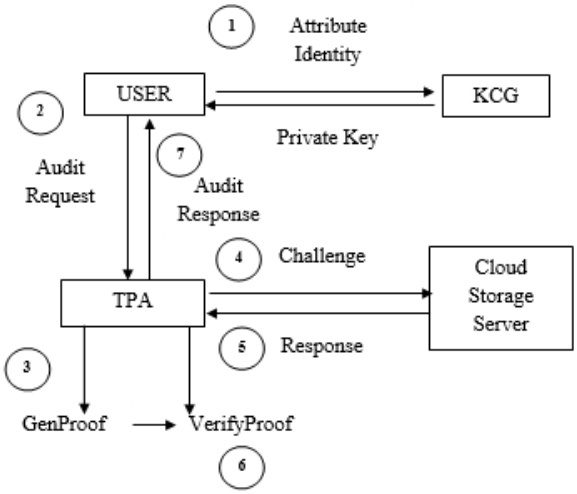

Fig.2. Proposed Architecture-Level-2

The building blocks of protocol architecture include:

- Cloud storage services
- Clients authentication
- Integrity check service

The protocol is made up of two execution processes that are completely different from each other. One of them is 'file storage process' and other is known as 'verification process'. Execution of the former is on demand and the client operates as a boot device. The latter begins with an integrity check service and the storage service is the cloud is verified by it in continuous operation.

The proposed public auditing is divided into two steps: Setup and Audit.

Setup: In this step, public parameters and secret parameters are initialized. KeyGen algorithm is executed for generation of public and private parameters. The data file, F, is first of all preprocessed and metadata is created using algorithm SigGen. The outcome of this algorithm is used for verification of metadata. After performing SigGen operation over F, the user then send data to cloud server to store it securely. Along with that, user sends the metadata to TPA for further verification audit on the stored data.

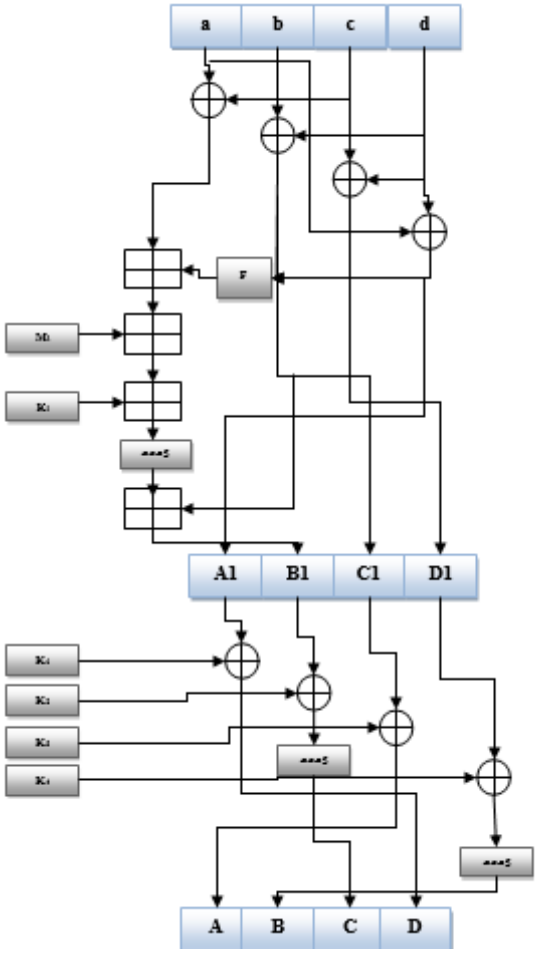

Fig.3. Process block of M-MD5

IV. RESULT ANALYSIS

The evaluation of the algorithm proposed focuses on four success indications, i.e. The Block Generation Time, the GenProof and the VerifyProof Time are visible.

The time it takes to create data blocks are block generation time.

Encryption time: it's time for data blocks to be encrypted.

GenProof Time is the time required for each encrypted data block to produce a digital signature or hash value.

VerifyProof Time is the time required to assessment the integrity test challenge.

A. Performance Evaluation

This section describes the performance evaluation of proposed methodology. The simulation analysis was performed on Intel Core i5 processor and an 8 GB Hard-discussing cloudsim using net beans platform.

The findings evaluated all Extract, Genproof and checkproof algorithms for time consumption. Table 1 shows the result analysis which is assessed using 1MB file variable size block. The size of the block ranges between 1KB and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 10, Issue 5, November 2020

100KB with an increase of 10KB Simulation takes place on encrypted data. Thus the table shows four time problems, such as block generation time, encryption time, gene-proof time and verifying time.

Table 1: The Performance Evaluation of Proposed Algorithm

Block Size	Block Generation Time (in ms)	Encryption Time (in ms)	GenProof Time (in ms)	Verify Proof Time (in ms)
1 KB	589	183243	553	1860
10 KB	152	151435	424	1747
20 KB	139	186325	412	1678
30 KB	133	151235	389	1526
40 KB	130	185369	367	1432
50 KB	128	142166	213	1357
60 KB	124	186782	203	1354
70 KB	122	177874	187	1314
80 KB	114	156705	146	1248
90 KB	110	142458	118	1194
100 KB	103	135661	106	1129

As seen in the Fig. 4, the extract time cost shows a linear increase in the attributes of the device with maximum m number.

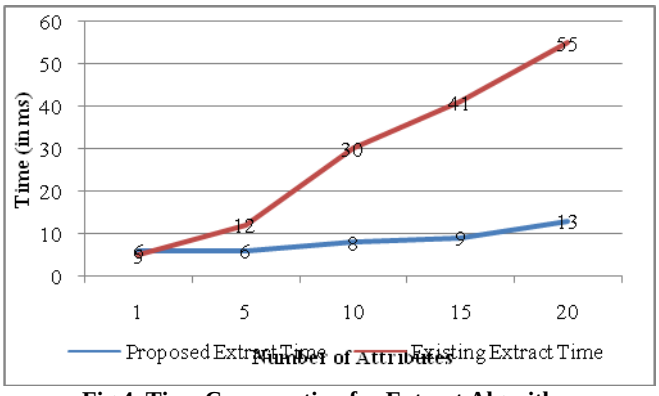

Fig.4. Time Consumption for Extract Algorithm

The Genproof algorithm with variable block size costs can be seen from table 2 and Fig.5. Data file for 1MB is divided into 10KB blocks of file up to 100KB blocks of file. The diagram shows that the gene-proof time complexity is reduced as the number of blocks increased.

Table 2: The Time consumption for GenProof algorithm of 1MB file

Block Size	Proposed GenProof Time (in ms)	Existing GenProof Time (in ms)
10 KB	553	3500
20 KB	424	2800
30 KB	412	2200
40 KB	389	1700
50 KB	367	1400
60 KB	213	1300
70 KB	203	1200
80 KB	187	1100
90 KB	146	1000
100 KB	118	1000

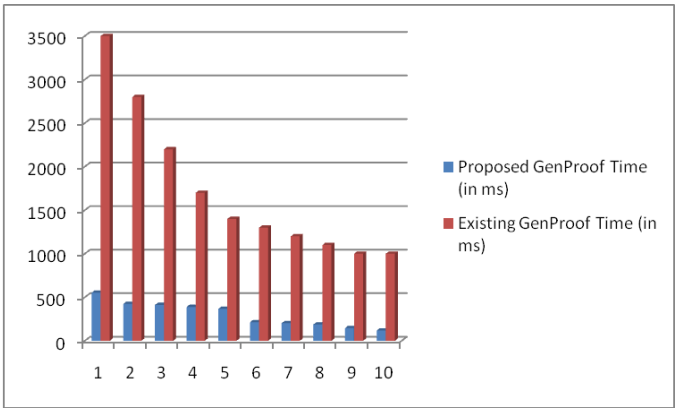

Fig.5. Time consumption for GenProof algorithm of 1MB file

Table 3: Time consumption for VerifyProof algorithm of 1MB file

Block Size	Proposed VerifyProof Time (in ms)	Existing VerifyProof Time (in ms)
10 KB	1860	18000
20 KB	1747	15000
30 KB	1678	12000
40 KB	1526	11000
50 KB	1432	10000
60 KB	1357	9000
70 KB	1354	9000
80 KB	1314	7000
90 KB	1248	7000
100 KB	1194	6000

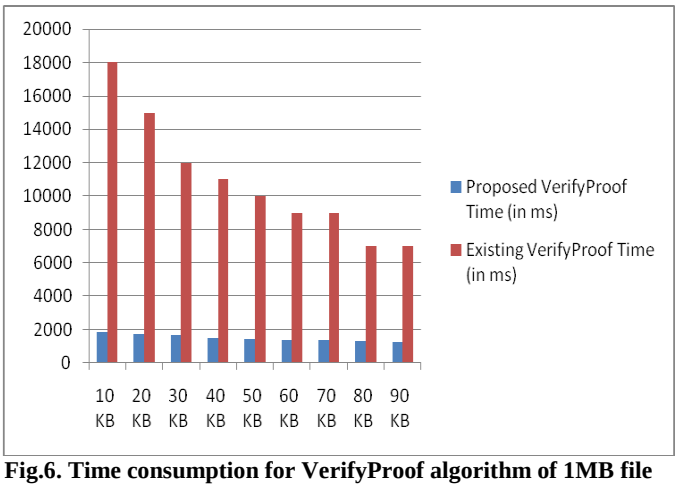

Fig.6. Time consumption for VerifyProof algorithm of 1MB file

As shown in Fig 6 and Table 3. The time expense of the variable block size Verifyproof algorithm. 1MB file is divided into 10KB blocks of file up to 100KB blocks of file. The diagram shows that the verifiable time complexity decreases as the number of blocks increases.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 10, Issue 5, November 2020

V. CONCLUSION

The study is proposed in combination with the Modification of the MD5 algorithm (MMD5) of the Elliptical Curve Modified RSA (ECMRSA) used for the verification of cloud attribute integrity. In the name of data owners, the Third Party Auditor (TPA) challenges the data server to ensure data file integrity. The auditor sends the audit report to the owner after assurance of the integrity of the data file.

The proposed auditing algorithm includes a public key-coding scheme with homomorphic algorithms that generates data file digital signature or hash values for coded files. With the increase in block size, processing costs increase in GenProof and VerifyProof as well as in the current work.

REFERENCES

[1] Jiguo Li, Hao Yan, Yichen Zhang, "Certificate less public integrity checking of group shared data on cloud storage" IEEE Transactions on Services Computing, pp:1-12, January, 2018.

[2] Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage" IEEE Transactions on Information Forensics and Security, Volume: 12, Issue 4, 2017, pp. 767 - 778.

[3] S. Suganya "Improving Cloud Security by Enhancing Remote Data Integrity Checking Algorithm" Innovations in Power and Advanced Computing Technologies (i-PACT) IEEE, pp:1-6, April 2017.

[4] T.Subha "Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security", International Conference on Advanced Computing (ICoAC), IEEE, pp: 55-60, January 2017.

[5] C. Sasikala "A Study on Remote Data Integrity Checking Techniques in Cloud", International Conference on Public Key Infrastructure and its Applications (PKIA), IEEE, pp: 43-48, Nov. 2017.

[6] Samundiswary. S "Public Auditing for shared data in cloud with safe user revocation", International conference of Electronics, Communication and Aerospace Technology (ICECA), IEEE, pp: 53-57, April, 2017.

[7] R.Swathi and T.Subha, "Enhancing Data Storage Security in Cloud using Certificateless Public Auditing", International Conference on Computing and Communications Technologies (ICCCT), IEEE, pp. 348-352 February, 2017.

[8] Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage". IEEE Transactions on Dependable and", IEEE Transaction on Emerging Topics in Computing, Vol. 14, No. 8, pp: 377-390, 2017.