Secure Cloud Data Audit using Protocol and Digital Signature Techniques

Prakash G L, Manish Prateek, Inder Singh

Abstract: Cloud computing is one of the important business models in the modern Information Technology. It provides various services (hardware, software) to the users with minimal interaction and low-cost. Storage service is one of the most useful services in cloud computing, which move data owners data from local computing system to the cloud. In this paradigm, once the data moves from the local computing system to the cloud, the data owner lost the physical control of the outsourced data on the cloud. So that, storage service creates data security challenges. Therefore, the integrity of the outsourced data has to be verified frequently using public or private verification method. In this paper we focus on two data security concern such as data confidentiality and remote data integrity on cloud storage system. In order to ensure the data integrity and reduce the data owners computational resources, in this work we have proposed a remote data integrity auditing methods such as Remote Data Audit using Protocol(RDAP) and Remote Data Audit using Digital Signature (RDADS) methods. To analyze the performance of the system, first, we define the single data owner on multiple servers and then multiple data owners on a single server for public data verification. Besides, these methods not only verify the integrity of data, but also detect the invalid data block during the verification process.

Keywords : Security, Authenticator, Public-auditing, Integrity, Storage as a Service

I. INTRODUCTION

Cloud computing is a new computing paradigm in Information Technology. The cloud computing is defined by National Institute of Standards and Technology (NIST) as enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) which can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. In this model, both hardware and software resources are delivered over the internet with the interaction between users and cloud service providers. There are three service models namely software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) which are implemented over private, public, hybrid or community deployment model. Despite several advantages, cloud computing has various issues and challenges, which need to be solved. Data privacy and security is one of the significant research areas in cloud computing. Cloud computing is one of the on-demand high-quality service delivery models with a lower cost. Amazon Web Service (AWS) is the most commonly used cloud service provider. They provide various services such as; Amazon Elastic Compute Cloud (EC2) an IaaS service, Amazon Elastic Beanstalk a PaaS service for hosting applications, Amazon Elastic Block Storage (EBS) and Amazon Simple Storage Service (S3) for storage, AWS Identity and Access Management (IAM) service for secure control access to AWS.

II. RELATED WORK

To ensure the data is only accessible by the authorized users and for end-to-end secure data transfer requires the efficient encryption and or decryption algorithm to the whole dataset before performing any further operations[2-11].

Jing-Jang Hwang et al. [4], has proposed a business model for cloud computing for data security using data encryption and decryption algorithms. In this method, cloud service provider is responsible for data storage and data encryption/decryption tasks, which takes more computational overhead for the process of data in a cloud server. The main disadvantage of this method is, there is no control of data for the data owner i.e, data owner has completely trusted with cloud service provider and he has more computational overhead

Cong Wang et al., [5], proposed a ranked keyword search over the outsourced cloud data for secure data access. In this method, the data owner send the data file along with a list of keywords in the data and its frequency to the cloud server.

The cloud server can derive the outsourced data using shared keywords and its frequency. So that, there is no privacy of the outsourced data from the untrusted cloud server. Besides, this the cloud service provider can also delete the rarely accessed data from the cloud storage for his storage space benefits.

Fatemi Moghaddam et al., [6] discussed the performance of six different symmetric key RSA data encryption algorithms in cloud computing environment.

They have proposed two separate cloud servers; one for data server and other for key cloud server and the data encryption and decryption process at the client side. The main drawback of this method is maintaining two separate servers for data security in the cloud, which creates more storage and computation over heads.

Manuscript published on November 30, 2019.

* Correspondence Author
Prakash G L*, School of Computer Science, University of Petroleum and Energy Studies, Email:prakshgl@ddn.upes.ac.in.
Manish Prateek, School of Computer Science, University of Petroleum and Energy Studies, Email:mprateek@ddn.upes.ac.in
Inder Singh, School of Computer Science, University of Petroleum and Energy Studies, Email:inder@ddn.upes.ac.in

To ensure that the data is only accessible for only authorized users and for end-to-end secure data the transfer requires the efficient encryption and/or decryption algorithm to the whole dataset before performing any further operations.

Further, it is very difficult to see the upcoming applications for the future without the proper use of algorithms. Also, several data security software needs to be developed for the privacy of the organizations data.

Mazhar Ali et al., [7] proposed a secure data sharing scheme in the cloud system that provides data confidentiality, secure data sharing and forward and backward data access control. The cost of data decryption is more as compared to the data encryption and maintaining multiple keys at third party server is not secure. Secure data sharing in the public cloud is an important issue in cloud computing. Xu et al., [8] addressed the issues of secured data sharing within the group and they proposed a certificate-less proxy re-encryption (CL-PRE) technique for secure data sharing in cloud storage system. In this technique, the data owner is encrypted data using a symmetric key algorithm and the symmetric key is encrypted using public key algorithm. The encrypted data and the key are uploaded to the cloud server, then the cloud server re-encrypt the encrypted key using the public key. This re-encryption is based on the complex bilinear pairing operations. The computational cost of pairing the operation is costlier than all the standard operations in the finite fields.

Seo et al., [9] proposed a mediated certificate-less encryption technique for data sharing the data on a public cloud without using bilinear pairing operations, which reduces the computational overhead. In this approach, the key pairs are generated by cloud server and distributes the public key to all the authorized data owners. The key management and partial decryption are done by the cloud server, user handling in easier but this is not suitable for the data security point of view because of untrusted cloud server. Besides, the cloud server handles the key management and decryption the operation, the computational overhead increases.

In public cloud, remote data integrity checking is an important security issue. Since the client's massive data is outside of their control, the client's data may be corrupted by the malicious cloud server regardless of intentionally or unintentionally. In this the section we present the recent remote data integrity verification scheme using protocol proposed by the researchers.

Ari Juels and Burton S. Kaliski Jr.[12], proposed the proofs of retrievability (PORs) scheme verifies the integrity of an archive or backup data file on a cloud server. The PORs has designed to handle large file using the cryptographic hash function. In POR protocols the cost of input/output data transmission, memory access, and storage requirements are independent to the length of the data during the data verification process. To verify small portion of the data file it takes more communication overhead due to downloading the entire file. Secondly, the auditor and verifier can derive the data file from the corresponding meta-data of the file. It is designed for the only static data file and which take more computational and transmission cost to verify the few blocks of data file. To solve data integrity issue for the data security in the cloud, recently several data auditing techniques are proposed [13], [14], [15]. These data auditing techniques allow data owner to check the cloud service provider stores data correctly. The PDP schemes reserve the integrity of outsourced data, but POR is not only preserved the integrity of the data and it recovers the partially corrupted data using error correcting codes. In this scheme the data integrity is verified by sampling method, so that both the method takes more storage and computational overheads.

Later on, H. Shacham and B. Waters in [16] propose the improved version of POR data auditing techniques such as private and public data verification. But in these schemes the private verification is only for data owner and also it is not supported for batch auditing. Subsequently, several PDP version of data auditing schemes [17], [18] are proposed to address the data privacy and security issues in the cloud. In this method, the data auditing is performed without retrieving the enter data from the Cloud servers, which is called a public data auditing scheme. In public auditing schemes cloud servers requires more computational and storage overheads for remote data auditing process.

In [18] proposed a delegable PDP scheme for remote data verification in this the method the data owner generates the delegation key for a verifier and stores on cloud server for data verification. But it does not support encrypted data so that there is no privacy guarantee for outsourced data. Afterward, Z. Mo et al.,[19] presented a proxy PDP model in which the data owner delegates the data-auditing task to a proxy server by sending the meta-data of the outsourced data. Due to insecure data auditing operations on unbelievable cloud server a designated verifier PDP schemes [20], [21], [22] are presented. In this method, the delegated verification is independent of the cloud server, which solves the data privacy problem, but it suffers from signature forgery attacks. Afterward, T su Yang Wu et al., [23] presented in non-repudiable PDP with designated verifier scheme to reduce the communication over between the verifier and cloud server and also address the forgery signature attacks.

III. PROBLEM STATEMENT

With the rapid development of the Information Technology, cloud storage service (such as AWS Simple Storage Service, Block Storage Service, Google Drive, DropBox , etc.,) is one of the most significant services in cloud computing in our daily life. It enables data owners to store the data in the remote cloud storage a system without the burden of local infrastructure, maintenance and is shared over the internet making it economically more viable. The data owner outsources the data to the remote storage server, the physical control of the data will be lost. So that the data confidentiality and integrity challenges have a significant influence on the data security and privacy of cloud storage systems. One major data security issue is how to ensure the confidentiality and integrity of the outsourced data on cloud storage server. For example, due to hardware or software failures, external or internal attacks, the cloud server may lose the owners data. However, because of the reputation of the service the cloud service provider can hide the administrative errors to the data owners.

A. *System model*

Consider a cloud storage system in Figure 1 consists of three computing entities such as; data owner, public verifier (data auditor), cloud service provider, and data users.

Cloud storage system permits the data owners to store, retrieve and share data with users. The detailed functions of these entities are as follows.

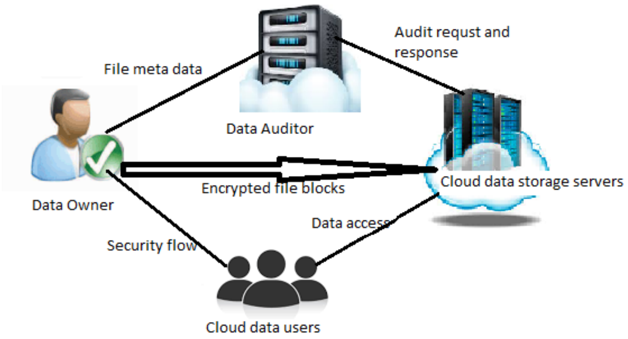


Fig. 1. Cloud system model

Data owner: The data owner can be any organization or an individual user who outsources the data to be stored in the data center. A unique identifier identifies each data owner.

Data Auditor/verifier: It is an entity who is trusted by all other entities of the system such as a cloud service provider (CSP) and data owner. The functions of the verifier is to verify whether the requested user is authorized or not and to check the correctness of outsourced data using the Decisional Diffe-Hellman method.

Cloud servers: It is a set of servers, which is managed by the cloud service provider to provide the storage service, which has massive compute and storage facility. It coordinates with the trusted third party to verify the authorized users and to retrieve the data from the cloud server to make them available for the authorized users on demand.

Data Users: An authorized user, who can access the outsourced data based on the request. The initial file setup and the auditing process has followed the following steps.

1. The data owner splits the file *(F)* into n blocks of size *s i.e* $Fi = m_{ij}$ where $i= 1$ to n and $j = 1$ *to s.* Each block is encrypted using encryption algorithm with a specific key and upload each block to the CSP. The data owner also sends the meta-data to the CSP.
2. The data owner then uploads the private key as well as the meta information of the uploaded file to the public verifier
3. The public auditor sends the data audit request message to the CSP regarding a specific file using its ID.
4. The CSP sends the _le tag for the requested file ID. Once the tag is verified, the public verifier shall query file blocks to the CSP. The CSP shall send the digital signatures of the requested blocks. Once the tag and all the signatures are verified, the public verifier shall confirm the validity of the file in CSP.
5. When the _le data blocks are verified by public verifier then it sends the status of the auditing to the data owner.

B. *Objectives*

In the proposed method, the following objectives are achieved for auditing outsourced data on cloud storage server.

1. Privacy of the data: To design a secured data auditing scheme, in which the verifier cannot derive owners data from its meta-data.
2. Flexible data auditing: To design a private or public data verification method, which can be applied based on the priority of outsourced data.
3. Block level data operation: To design a secure block level encrypted data operations.
4. Lightweight overhead: To optimize the storage, computation, and communication overhead to perform the data auditing on a cloud server.

IV. PROPOSED ALGORITHMS

A. *Basic Auditing Scheme*

The basic data integrity verification scheme consists of three stages such as; key generation, meta-data generation, and data audit.

Key Generation: It is an entity, which takes the input as security parameter *(k)* and the data owner identifier *(id)* and generates the public parameters, secret key, public key, and owners private key *(pk_{id}).*

Meta-data Generation: To generate the meta-data for a given file Fi of the owner id, the meta-data generator takes input as owners private key pk_{id} and the file *Fi* as input and generates the signature of file blocks interns of block-tag pair.

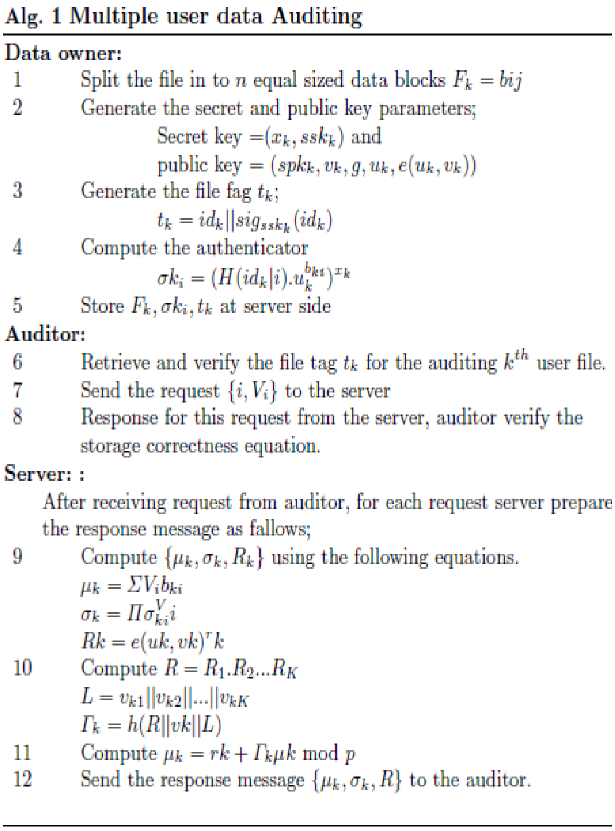
Data Audit: The data auditing process consists of five steps of the request, response, and verification among the verifier, cloud service provider and cloud server.

1. Verifier sends the challenge request to the cloud service provider for verification of the selected number of data blocks stored on cloud server.
2. The combiner searches the requested data blocks meta-data from the metadata table and then distribute the request to the corresponding cloud server.
3. After receiving the responses from the cloud servers, the cloud service provider combines all the responses.
4. cloud service provider sends the final combined response to the verifier.
5. The verifier verifies the response message using bilinear map operation. If the response is valid, verifier confirms data blocks are not modified, otherwise, he declares data blocks are modified.

B. *Remote Data Audit using Protocol(RDAP)*

In this section we proposed a public auditing for single data owners file by utilizing HLA scheme for proof of retrievability of outsourced data file. The design steps for this method such as key generation, file setup and public auditing are described as follows.

The detail procedure for this auditing is explained in Algorithm 1. Let *k* is the number of data owners in the system and each owner has data file $F_k = \{ b_{ij} \}$ store on cloud server and each file has n number of data blocks. To audit the outsourced these files stored on cloud server using batch processing the detailed procedure as follows.

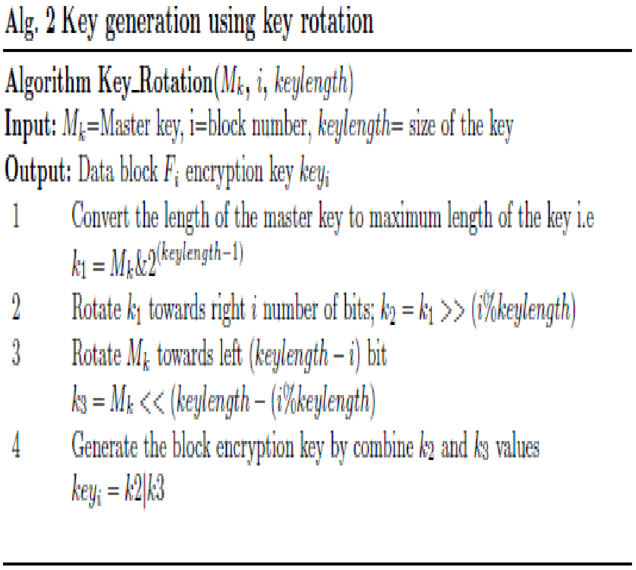


Alg. 1 Multiple user data Auditing

```
Data owner:
1   Split the file in to $n$ equal sized data blocks $F_k = bij$
2   Generate the secret and public key parameters;
        Secret key =$(x_k, ssk_k)$ and
        public key = $(spk_k, v_k, g, u_k, e(u_k, v_k))$
3   Generate the file fag $t_k$;
        $t_k = id_k||sig_{ssk_k}(id_k)$
4   Compute the authenticator
        $\sigma k_i = (H(id_k|i).u_k^{b_{ki}})^{x_k}$
5   Store $F_k, \sigma k_i, t_k$ at server side
Auditor:
6   Retrieve and verify the file tag $t_k$ for the auditing $k^{th}$ user file.
7   Send the request $\{i, V_i\}$ to the server
8   Response for this request from the server, auditor verify the
    storage correctness equation.
Server: :
  After receiving request from auditor, for each request server prepare
  the response message as fallows;
9   Compute $\{\mu_k, \sigma_k, R_k\}$ using the following equations.
    $\mu_k = \Sigma V_i b_{ki}$
    $\sigma_k = \Pi \sigma_{ki}^{V} i$
    $Rk = e(uk, vk)^r k$
10  Compute $R = R_1.R_2...R_K$
    $L = v_{k1}||v_{k2}||...||v_{kK}$
    $\Gamma_k = h(R||vk||L)$
11  Compute $\mu_k = rk + \Gamma_k \mu k \bmod p$
12  Send the response message $\{\mu_k, \sigma_k, R\}$ to the auditor.
```

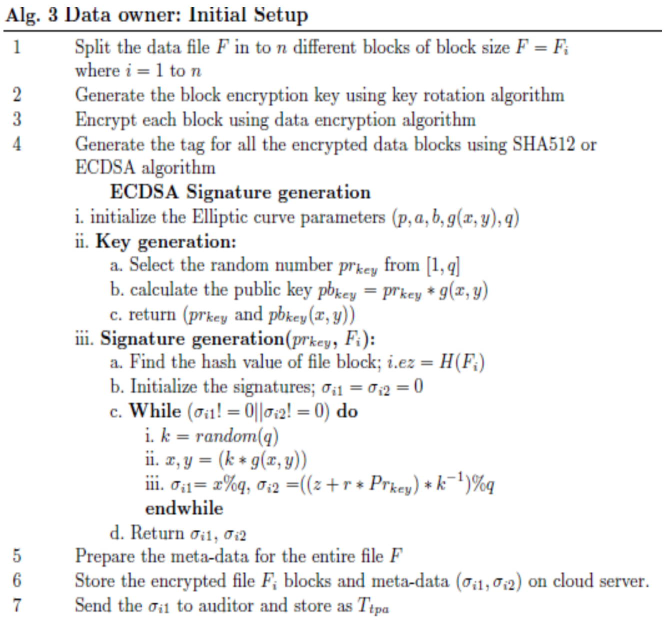
C. *Data Audit using Digital Signatures(RDADS)*

This section presents the detailed design and algorithms for remote data checking using Elliptic curve digital signature method in the cloud. The proposed method consists of initial file setup and data audit phase. The detail algorithms for data verification as presented in the algorithms 2,3 and 4.



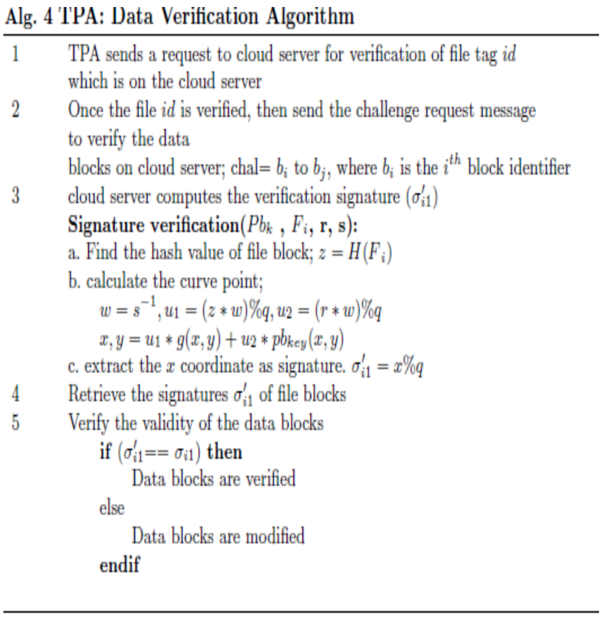
Alg. 2 Key generation using key rotation

```
Algorithm Key_Rotation($M_k$, $i$, $keylength$)
Input: $M_k$=Master key, i=block number, $keylength$= size of the key
Output: Data block $F_i$ encryption key $key_i$
1   Convert the length of the master key to maximum length of the key i.e
    $k_1 = M_k \& 2^{(keylength-1)}$
2   Rotate $k_1$ towards right $i$ number of bits; $k_2 = k_1 >> (i\%keylength)$
3   Rotate $M_k$ towards left $(keylength - i)$ bit
    $k_3 = M_k << (keylength - (i\%keylength)$
4   Generate the block encryption key by combine $k_2$ and $k_3$ values
    $key_i = k2|k3$
```



Alg. 3 Data owner: Initial Setup

```
1   Split the data file $F$ in to $n$ different blocks of block size $F = F_i$
    where $i = 1$ to $n$
2   Generate the block encryption key using key rotation algorithm
3   Encrypt each block using data encryption algorithm
4   Generate the tag for all the encrypted data blocks using SHA512 or
    ECDSA algorithm
        ECDSA Signature generation
    i. initialize the Elliptic curve parameters $(p, a, b, g(x, y), q)$
    ii. Key generation:
        a. Select the random number $pr_{key}$ from $[1, q]$
        b. calculate the public key $pb_{key} = pr_{key} * g(x, y)$
        c. return $(pr_{key}$ and $pb_{key}(x, y))$
    iii. Signature generation($pr_{key}$, $F_i$):
        a. Find the hash value of file block; $i.ez = H(F_i)$
        b. Initialize the signatures; $\sigma_{i1} = \sigma_{i2} = 0$
        c. While $(\sigma_{i1}! = 0||\sigma_{i2}! = 0)$ do
            i. $k = random(q)$
            ii. $x, y = (k * g(x, y))$
            iii. $\sigma_{i1}$= $x\%q$, $\sigma_{i2}$ =$((z + r * Pr_{key}) * k^{-1})\%q$
            endwhile
        d. Return $\sigma_{i1}$, $\sigma_{i2}$
5   Prepare the meta-data for the entire file $F$
6   Store the encrypted file $F_i$ blocks and meta-data $(\sigma_{i1}, \sigma_{i2})$ on cloud server.
7   Send the $\sigma_{i1}$ to auditor and store as $T_{tpa}$
```



Alg. 4 TPA: Data Verification Algorithm

```
1   TPA sends a request to cloud server for verification of file tag $id$
    which is on the cloud server
2   Once the file $id$ is verified, then send the challenge request message
    to verify the data
    blocks on cloud server; chal= $b_i$ to $b_j$, where $b_i$ is the $i^{th}$ block identifier
3   cloud server computes the verification signature $(\sigma'_{i1})$
    Signature verification($Pb_k$ , $F_i$, r, s):
    a. Find the hash value of file block; $z = H(F_i)$
    b. calculate the curve point;
        $w = s^{-1}, u_1 = (z * w)\%q, u_2 = (r * w)\%q$
        $x, y = u_1 * g(x, y) + u_2 * pb_{key}(x, y)$
    c. extract the $x$ coordinate as signature. $\sigma'_{i1} = x\%q$
4   Retrieve the signatures $\sigma'_{i1}$ of file blocks
5   Verify the validity of the data blocks
        if $(\sigma'_{i1} == \sigma_{i1})$ then
            Data blocks are verified
        else
            Data blocks are modified
        endif
```

V. PERFORMANCE ANALYSIS

This section presents the simulation results of the proposed RDADS [24] using ECDSA algorithm techniques. The performance of the proposed remote data auditing methods computation and communication overheads during initial file setup and data audit phases are presented in the following section.

A. Simulation setup

To evaluate the performance of our proposed algorithms are implemented using Python programming language with built-in cryptography functions in Python library. The simulation result is tested on Amazon Web Service EC2 virtual machines(VM).

B. Communication Cost

The communication cost in the initial file setup is the same order of growth in all the proposed data auditing methods.

Retrieval Number: D6970118419/2019©BEIESP
DOI:10.35940/ijrte.D6970.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

But the communication cost between TPA and cloud service provider varies in the data audit phase. So that, we compare the computation cost for data audit in the proposed method.

Consider a batch auditing with K data owners and C cloud servers, a number of challenging blocks in each task is t, and the size of each block is s. The total cost during the challenging phase is *O(ts)*, so that the communication cost for proof generation depends on the number of challenging blocks and size of each block. Finally, the server sends an only proof message to the TPA, so that the communication cost from CSP to TPA is *O(1)*. The total communication cost in the auditing phase is the sum of the challenging task, proof generation and proof communication between CSP and TPA i.e, *O(1) + O(ts) + O(1) = O(ts).*

C. Computation Cost

Due to the large data file, we use the sampling auditing method to verify the outsourced data in the cloud. The computation cost of the TPA and CSP to audit data blocks on a single server and multiple data owners is presented in the following section.

The performance analysis of the RDASDS and RDAP methods interns of computation cost is analyzed using the following parameters; Signature generation cost, File setup and upload time, Data block verification time, Detection of the modified data block, CSP vs TPA computation time, RDAP vs RDADS signature and data verification.

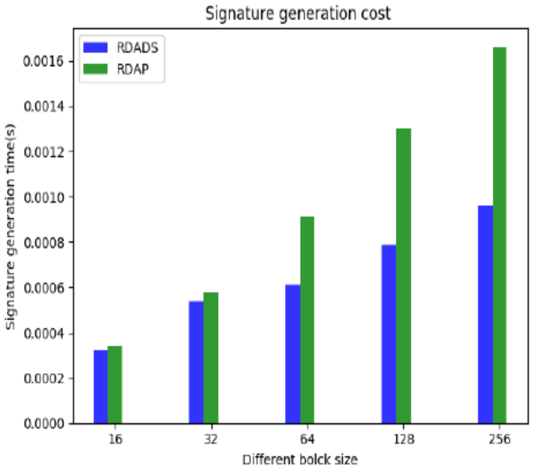


Fig. 4. Signature generation cost for different blocks

Signature Generation Cost: The computational comparison between RDAP using a linear authenticator and RDADS using elliptic curve signature generation of a 10MB data file with different block size as shown in Figure 4.

In Figure 4, the X-axis represents the different data block sizes in terms of Kilo Bytes and Y-axis represents the signature generation cost in seconds(s). The simulation result shows that the computational overhead for data block signature generation of RDADS method has a lower order of growth than RDAP method. For smaller sized data blocks signature generation cost of both the methods has same growth order. But for the larger sized data blocks, RDAP has a higher order of growth order than RDADS. This change is due to the number of computation operations for a signature generation in RDAP is more expensive than RDADS method.

File Setup and Upload Time: Figure 5 shows the computational and communication costs for signature generation and storing of data blocks in a cloud server in the initial file setup phase.

In Figure 5, the X-axis represents the different number of the 256KB data block(different file sizes) and Y-axis represents the file setup cost in seconds(s).

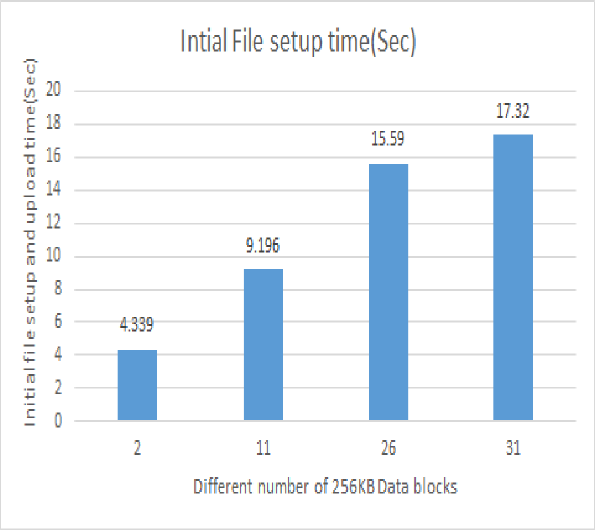


Fig. 5. Initial File setup and Upload time(sec)

Apparently, it shows that, the computational overhead of initial file setup for larger file is better than the smaller file. The communication overhead between data owner and cloud service provider of RDADS and RDAP are same in the initial setup phase.

Data Audit Time: The computational cost comparison between RDADS and RDAP method for audit different number of 256KB data blocks challenging task as shown in Figure 6.

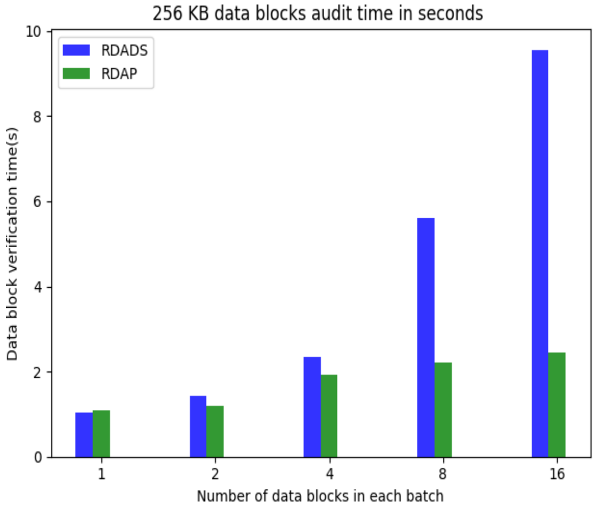


Fig. 6. Data block verification cost

In Figure 6, X-axis represents the different number of data blocks in each batch and Y-axis represents the data verification cost between TPA and CSP. The result shows that for the larger batch size RDADS method takes more cost than the RDAP method. This changes due to the expensive elliptic curve points operations are involved in RDADS during the data verification phase. But in the security point of view, RDADS method is better than the RDAP method.

Modified Data Block Audit Time: The performance analysis of the RDADS and RDAP for corrupted data block verification as shown in Figure 7. As compared to RDAP method of data auditing, the RDADS method is higher computation cost for larger batch size, because RDADS contains expensive el- liptic curve points operations in the auditing phase.

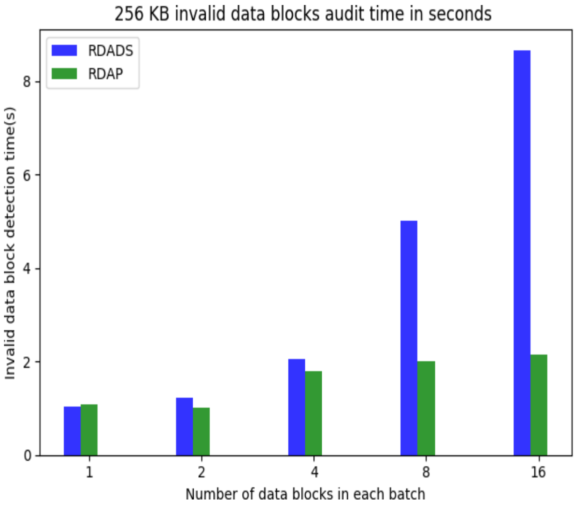


Fig. 7. Incorrect verification blocks time

Depending on the trust between the data owner and CSP the frequency of auditing is decided. The TPA select the t number of the data block in each auditing task to verify the integrity of data blocks on the cloud. The probability of detection on any corrupted data block sector s is defined as *Pr(t, s) = 1 (1 ρ)ts*, where ρ is the probability of data corrupted on cloud and t is the auditing batch size.

Computation Cost Comparison between CSP and TPA: As Figure 8 and Figure 9, shows that audit time comparison between TPA and CSP to verify the outsourced 256KB and 50KB data blocks using RDADS method respectively.

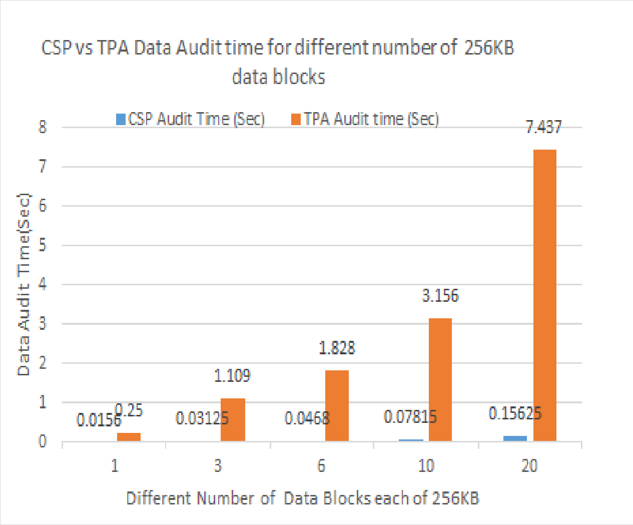


Fig. 8. CSP and TPA 256KB Data Blocks Audit Time(sec)

In Figure 8, X-axis represents the different batch sizes of 256KB blocks and Y-axis represents the computation overhead in seconds. The simulation result shows that, TPA takes negligible computation cost than CSP, because of the TPA delegate the auditing task to the CSP so that CSP computation overhead varies for different bath size.

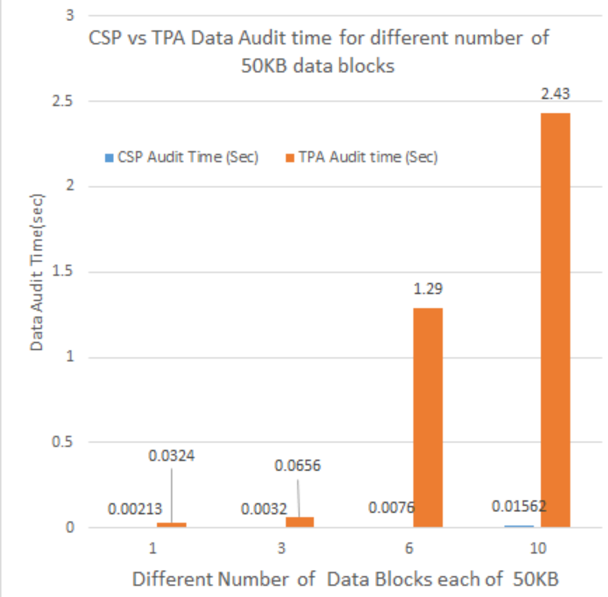


Fig. 9. CSP and TPA 50KB Data Blocks Audit Time(Sec)

The computation overhead comparison between TPA and CSP for 50KB of data blocks audit as shown in the Figure 9. As compared to 256KB of data blocks, TPA takes same computation cost as 50KB blocks. But the CSP computation cost varies based on the batch size in both the cases.

Computation Cost Comparison between RDAP and RDADS: In Figure 10, depicts the comparison on data blocks signature generation time using RDAP and RDADS method for different file size with 256KB of data blocks. It is easily observed that RDADS method has less computation time compared to RDAP method. This difference is due to RDADS algorithm takes less number of operations to generate the block signature compared to RDAD method.

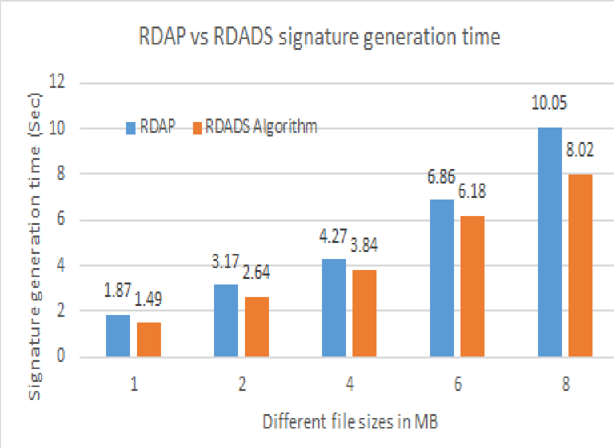


Fig. 10. RDAP vs RDADS Signature generation time for 256KB blocks

Figure 11, shows, the comparison of data blocks audit computation cost using RDAP and RDADS method for a different number of data blocks each of 256KB. It is easily observed that RDADS method has less computation cost for the smaller number of data blocks compared to RDAP method and more computation cost for the larger number of data blocks. This change is due to RDADS Elliptic curve method points complex operations is increases for the larger blocks. But for the security point of view, RDADS algorithm is better to secure data audit method compared to RDAP method.

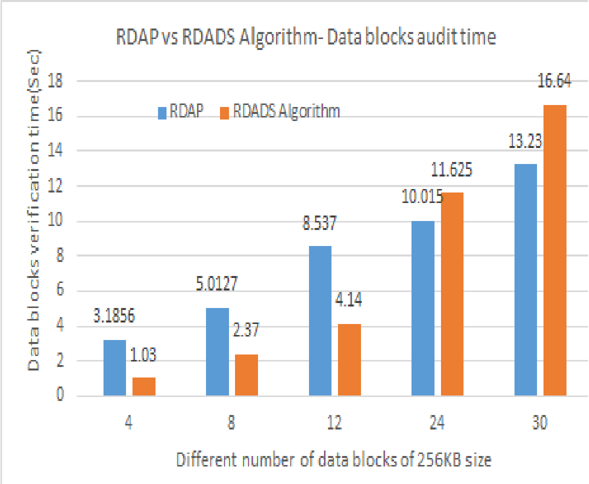


Fig. 11. RDAP vs RDADS 256KB data blocks verification time

VI. CONCLUSIONS

In order to fulfill this objective, we have proposed a secure public data auditing techniques using protocol and digital signature scheme. Based on the comparison of our digital signature data auditing scheme benefits from security level and minimum computational overhead. In addition, our proposed method is de- signed for constant storage and computational support for each auditing task. The proposed data auditing scheme utilizes the block level data auditing with masking response message on encrypted data to provide data privacy to untrusted entities. The digital signature method provides acceptable competition and storage communication overhead at server side due to light-weight elliptic curve points operations. Regarding the data privacy and security of the proposed remote data auditing scheme on an untrusted cloud service provider, several other security issues are still a challenging task in cloud computing. For future perspective, our proposed key rotation symmetry data encryption process is relying on personalized symmetric key and it takes heavy computational overhead to decrypt the data. So that, generating an identity based deciphering key is an alternative solution. In cloud computing, more than 60% of resource-constrained devices are used to share data over the internet. The communication cost of our proposed data auditing schemes affecting the bandwidth consumption due to the location of the auditor and the location of storage . So that, we can implement a customizable data owners auditor to evaluate the impact of data owners location. We have shown the data privacy performance of data auditing schemes within a same cloud service providers.

To conclude, our main objective was to address the cloud data privacy and security issues using data confidentiality and remote data integrity verification. We have provided a protocol and digital signature based on cryptography approaches to address the data security issues in the cloud. Finally, we believe that cloud data storage security challenges are not limited and also it is an important research area in cloud computing for secure data sharing.

REFERENCES

1. Badger, L., Grance, T., Patt-Corner, R., and Voas, J, “Draft cloud computing synopsis and recommendations,” in National Institute of Standards and Tech- nology (NIST) Special Publication, http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf, pp. 800–146, 2011.
2. Ayad Barsoum and Anwar Hasan, “Enabling dynamic data and indirect mutual trust for cloud computing storage systems,” in IEEE Transactions on Parallel and Distributed Systems, 2012.
3. Ayad Ibrahim Abdulsada, Aqeel N. Mohammad Ali, Zaid Ameen Abduljabbar, Haider Sh.Hashim, “Secure image retrieval over untrusted cloud servers,” Inter- national Journal of Engineering and Advanced Technology (IJEAT), vol. 3, no. 1, pp. 140–147, 2013.
4. Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, Chien-Hsing Wu,, “A business model for cloud computing based on a separate encryption and decryption service,” in International Conference on Information Science and Applications (ICISA), pp. 1–7, 2011.
5. C. Wang, N. Cao, K. Ren, and W. Lou, “Enabling secure and efficient ranked keyword search over outsourced cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, 2012.
6. Fatemi Moghaddam F, Karimi O, Alrashdan M T, “A comparative study of ap- plying real-time encryption in cloud computing environments,” in IEEE 2nd In- ternational Conference onCloudNetworking(CloudNet), pp. 185–189, 2013.
7. Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, “Sedasc: Secure data sharing in clouds,” in IEEE SYSTEMS JOURNAL, vol. 11, no. 2, pp. 395–404, 2017.
8. L. Xu, X. Wu, and X. Zhang, “CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud,” in Proceeding of 7th ACM Symposium Information Computing Communication and Security, pp. 87–88, 2012.
9. S. Seo, M. Nabeel, X. Ding, and E. Bertino, “ CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud,” in IEEE Trans. Knowl. Data Eng., vol. 26, no. 9, pp. 2107–2119, 2013.
10. Y. Chen and W. Tzeng, “Efficient and provably-secure group key management scheme using key derivation,” in IEEE 11th International Conference on Trust- Com, pp. 295 – 302, 2012.
11. R. A. Sana Belguith, Abderrazak Jemai, “Enhancing data security in cloud computing using a lightweight cryptographic algorithm,” in IEEE ICAS 2015 : The Eleventh International Conference on Autonomic and Autonomous Systems, 2015.
12. Juels and B. S. Kaliski, Jr, “Pors: Proofs of retrievability for large files,” vol. 5, pp. 584 – 597, 2007.
13. G. Ateniese et al.,, “Provable data possession at untrusted stores,” in Proceeding 14th ACM Conference on Computing Communication and Security, pp. 598 – 609, 2007.
14. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proceeding of 4th International Conference on Secu- rity, Privacy, Communication Networks, p. 9, 2008.
15. A.Juels and B.S. Kaliski Jr., “Pors: Proofs of retrievability for large files,” in 14th ACM Conference on Computer and Communications Security, pp. 584 – 597, 2007.
16. H. Shacham and B. Waters, “Compact proofs of retrievability,” in in Advances in Cryptology - ASIACRYPT, Heidelberg, Germany: Springer, vol. 5350, pp. 90 – 107, 2008.
17. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Pors: Proofs of retrievability for large files,” in Proceeding of ACM Workshop Cloud Computing, Security, vol. 5, no. 3, pp. 31 – 42, 2010.
18. S.-T. Shen and W.-G. Tzeng, “Delegable provable data possession for remote data in the clouds,” in Proceeding of ICICS, pp. 93 – 111, 2011.
19. Z. Mo, Y. Zhou, S. Chen, and C. Xu, “Enabling non-repudiable data possession verification in cloud storage systems,” in Proceeding of IEEE 7th International Conference on Cloud Computting (CLOUD), pp. 232 – 239, 2014.
20. Y. Ren, J. Shen, J. Wang, and L. Fang, “Analysis of delegable and proxy provable data possession for cloud storage,” in Proc. 10th IEEE International Conference on Intelligence Information Hiding Multimedia Signal Process(IIH-MSP), pp. 779– 782, 2014.
21. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” in International JournalofInternetTechnologies, vol. 16, no. 2, pp. 317 – 323, 2015.
22. J. Zhang, P. Li, and M. Xu, “On the security of an mutual verifiable provable data auditing in public cloud storage,” in International Journal of Networks Security, vol. 19, no. 4, pp. 605 – 612, 2017.

23. Tsu Yang Wu, Yuk-Min Tseng, Sen-Shan Huang, and Y-Chen Lai, “Non-repudiable provable data possession scheme with designated verifier in cloud storage systems,” in IEEE Journal of Access, vol. 5, pp. 19333–19341, 2017.
24. Prakash G L, Manish Prateek and Inder Singh, “Performance analysis of cloud data verification using MD5 and ECDSA method,” Data Science and Analytics, Springer Singapore, vol. 799, pp. 616–628, 2018.

AUTHORS PROFILE

Dr. Prakash G L is an Assistant Professor with the School of Computer Science at University of Petroleum and Energy Studies, Dehradun, India. He received his B.E and M.E degrees in Computer Science and Engineering from Bangalore University, Bangalore. He did his Ph.D program in the area of data storage and security in Cloud Computing from University of Petroleum and Energy Studies in the year 2018. He has published more than 7 international journals and 15 international conference papers.

Dr. Manish Prateek did his Undergrad and Post Grad degree in the field of Computer Science from South West State University, (formerly known as Kursk State Technical University), Russia, in 1996. Since then he worked at different level in the IT industry in India as well as in Middle East. He did his PhD in the area of Manufacturing & Robotics and was awarded the degree in the year 2007. In 2005 he took up his career into technical education and started as Associate Professor and Head, Dept. of Information Technology at GRIET Hyderabad and later became a full Professor at the age of 36.

Currently he is working as Professor & Dean at UPES, Dehradun. His area of research includes Robotics and Automation, Image Processing and Patter Recognition, Cyber Security, Machine Vision etc. So far, more than 40 research papers have been published by him in different International Journals. He is also a recipient of Lifetime Achievement Award for his contribution in the field of education and research by the prestigious scientific society Pentagram Research Centre. He is also a member at the prestigious International Federation for Systems Research (IFSR), Austria

Dr. Inder Singh, M.Sc.(IT), M. Tech. (IT), Ph.D., Microsoft Certified Professional, IBM DB2 certified, e-commerce certification from Asset International, Dell EMC?s Certified Data Science Associate. He is an Assistant Professor (S.G.) at School of Computer Science and Engineering, UPES, Dehradun. He has over 16 years of working experience. He has started his career as Systems Administrator and switched to teaching profession after 6 years.

His area of research includes Computer Networks, Cloud Computing and Virtualization, and Data Science. So far, he has published and presented more than 18 research papers in different International Journals and conferences.

Retrieval Number: D6970118419/2019©BEIESP
DOI:10.35940/ijrte.D6970.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)