ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

DESIGN A PRIVACY-PRESERVATION APPROACH USED IN PUBLIC AUDITING FOR REGENERATING-CODE-BASED CLOUD STORAGE

Research Scholar - **BANOTH ANANTHARAM**[1]

Department of COMPUTER SCIENCE & ENGINEERING, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore,MP,India

Research Guide - **Dr.Neeraj Sharma**[2]

Department of COMPUTER SCIENCE & ENGINEERING, School of Engineering , Sri Satya Sai University of Technology & Medical Sciences, Sehore,MP,India

Research Co-Guide - **Dr. B.Kavitha Rani** [3]

Department of COMPUTER SCIENCE & ENGINEERING, CMR Technical Campus, Hyderabad, Hyderabad, Telangana 501401.

Abstract- Cloud computing is one of evolving technology nowadays, giving versatile services. However, secure information sharing is vulnerable to cloud computing. With cloud storage services, customers can remotely keep their information to the cloud and recognize the data sharing with others. Access management is a troublesome task to share sensitive information on cloud servers. Remote data integrity auditing is proposed to guarantee the integrity of the information stored in the cloud. The cloud data might contain some sensitive information it should no longer be exposed to others when the cloud report is shared. Encrypting the entire shared file can recognize the sensitive data hiding; however, it will make this shared report not able to be utilized by others. At pick time the server not able to serve the entire request at the time. In order to address this problem, we propose a remote data integrity auditing scheme and secure Data sharing with time constraints mechanism in Cloud Computing to protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this research, author proposes a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating-code-based cloud storage.

Keywords-Cloud storage, Third-Party Auditor (TPA), Data Integrity Auditing, Privacy-Preserving, Public Auditing, Regenerating-Code.

1. INTRODUCTION

The data shared in cloud servers, usually carries customer's sensitive/private data and needs to be nicely protected. Also, it is crucial to verify the integrity of information. It is a big challenge to defend the privacy of shared records in cloud, especially in cross cloud and big data environment. Where huge data consists of excessive volume, high range and excessive veracity records units with high pace processing requirement. Big data gives the superb opportunities and transformable capability for diverse areas inclusive of e-commerce, health care industry manufacturing, social network and academic services. In order to satisfy this mission, it is essential to layout an answer to provide user-described authorization length and also provide excellent grained get right of entry to control at some point of this duration. It is also important to provide the integrity through comparing both the signatures to confirm whether the data stored on cloud is tampered or not. It verifies the integrity of records on call for of the customers.With cloud storage services, users can remotely save their data to the cloud. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In a few common the sensitive data should not be uncovered to others when the cloud file is shared.

1.1 Problem Statement

Many mechanisms dealing with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now. The most significant work among these studies are the PDP (provable data possession) model and POR (proof of retrievability) model, which were originally proposed for the single-server scenario respectively.Considering that files are usually striped and redundantly stored across multi-servers or multi-clouds, explore integrity verification schemes suitable for such multi-servers or multi-clouds setting with different redundancy schemes, such as replication, erasure codes, and, more recently, regenerating codes. Separately and independently extended the single-server CPOR scheme to the regenerating code scenario; designed and implemented a data integrity protection (DIP) scheme for FMSR-based cloud storage and the scheme is adapted to the thin-cloud setting.

1.2 Background

Cloud computing is a style of computing where anyone can easily obtain and access the computing resources anytime. It is cheaper and simple to use and work with it. Cloud computing permits global, expedient, on-demand service network access to a shared pool of configurable computing services (e.g. networks, servers, storage, applications, and services) which can be quickly delivered with nominal managing efforts or service provider collaboration. Making use of the cloud saves both users time and money. The term cloud is widely used as a metaphor on the Internet, so it is the type of Internet based computing, where different amenities such as servers, storage and applications are distributed to an organization's computers and devices connected to the Internet.

1.3 Motivation

As an emerging network storage technology, cloud storage has been extended and developed in cloud computing. Cloud computing systems are transformed into cloud storage systems when the core of computing and processing is to store and manage massive data. In simple terms, cloud storage is an emerging solution that puts storage resources on the cloud for people access.The user can access data on the cloud easily through any connected device whenever and wherever. Through data storage and sharing services in cloud computing, group members can share data in the form of a group. As a member of a group, users can not only access the shared data, but also modify the shared data.

1.4 Scope of the Research

The scope of this project is that author focus on the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy. To fully ensure the data integrity and save the users' computation resources as well as online burden, we propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration (of failed data blocks and authenticators) are implemented by a third-party auditor and a semi-trusted proxy separately on behalf of the data owner.

1.5 Objectives of the paper

1. To propose a public auditing scheme for the regenerating-code-based cloud storage.
2. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model.

3. To design a novel public verifiable authenticator, this is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden.
4. To develop encode coefficients with a pseudorandom function to preserve data privacy.
5. To design Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating-code-based cloud storage.

2. REVIEW OF LITERATURE

NoshinaTariq(2019)[1],This study examines potential security and privacy challenges in fog-enabled IoT system. The main goal of this work is to provide insight on securing big data generated by fog-enabled IoT applications. We started with different IoT applications that generate massive amount of data followed by fog computing architecture, fog-enabled IoT applications security requirements and fog computing security challenges. We studied different existing state-of-the-art security and privacy approaches to map these challenges along with their limitations. We also considered the block chain as an emerging security solution along with the potential benefits to address security issues in fog-enabled IoT domain accompanied by some existing block chain solutions in IoT systems.

XinDong(2014)[2],This paper is aimed a dependable and secure cloud data sharing service that allows users dynamic access to their data. In order to achieve this, we propose an effective, scalable and flexible privacy preserving data policy with semantic security, by utilizing cipher text policy attribute based encryption (CP-ABE) combined with identity-based encryption (IBE) techniques. In addition to ensuring robust data sharing security, our policy succeeds in preserving the privacy of cloud users and supports efficient and secure dynamic operations including, but not limited to, file creation, user revocation and modification of user attributes.

YunchuanSun(2014)[3], Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers.

L. Malina(2015)[4], Anovel security solution for privacy-preserving cloud services. We propose the non-bilinear group signatures scheme to ensure the anonymous authentication of cloud service clients. Our novel solution offers user anonymity in the authentication phase, data integrity and confidentiality and the fair revocation process for all users. Users use tamper resistant devices during the generation and storing of user keys to protect against collusion attacks. Our authentication phase, which is based on the non-bilinear group signature scheme, is more efficient than related solutions on the client side and also on the server side due to missing expensive bilinear pairing operations and fewer exponentiation operations.

Lo'ai A. Tawalbeh(2019)[5], the organizations efficiency. These trends include cloud and mobile cloud computing but along with these technologies there are many associated challenges that should be taken in consideration such as users privacy and data security. Then we studied the possibility of applying new countermeasures against security threats. In particular, we presented four non-traditional encryption techniques and analyzed the visibility of using them in terms of performance parameters to secure big data in cloud environments, namely, format preserving encryption, homomorphic encryption, verifiable computation, and secure multi-party computations.

ZhongboShi(2014)[6], This study examinesa novel scheme for coding photo albums in clouds. Utilizing feature-based measurements instead of pixel-wise ones to evaluate and exploit interim age correlations. Unlike previous schemes for image set compression, we adopt content-based feature matching which is invariant to scale and rotation and less sensitive to illumination changes for both correlation estimation and redundancy reduction.

RajkumarBuyya(2013)[7], The main part of this paper Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements regardless of where the services are

hosted. Several computing paradigms have promised to deliver this utility computing vision. Cloud computing is the most recent emerging paradigm promising to turn the vision of "computing utilities" into reality. Cloud computing started with a risk-free concept: Let someone else take the ownership of setting up of IT infrastructure and let end-users tap into it, paying only for what is been used. A service offering computation resources is frequently referred to as Infrastructure as a Service (IaaS) and the applications as Software as a Service (SaaS).

IsranaHossainArka(2014)[8], This study examinesindependent cloud based collaborative medical image storage and mobile viewer assisted with effective compression and decompression technique with unique security structure design. The proposed design has considered deep technology exploitation to offer medical image access via mobile devices by considering all the current constraints in terms of storage, image clarity and security. The proposed architecture allows both patient and medical practioners to have a cost effective approach in disease management and treatment process.

SajidaKarim(2020)[9],The main part of this paperFace book compressed videos that decrease the quality of the video, make more blurry and noisy as compared to other social clouds, and signifies the relation existing in video sequences, respectively. These all metrics are robust evident in the compressed video for Qzone and Tumblr videos; Tumblr adds low noise rate as compared to Qzone, and both provide the best quality as compared to other social cloud videos and metrics. Therefore, we can conclude that Qzone and Tumblr metrics capture the high quality of video even in the lowest transmission bit-rates, and increased QoE and provided the QoS.

H. B. Kekre(2016)[10],This study examinessimpler image compression technique using vector quantization and hybrid wavelet transform. Hybrid wavelet transform is generated using Kronecker product of two different transforms. Image is converted to transform domain using hybrid wavelet transform and very few low frequency coefficients are retained to achieve good compression. Vector quantization is applied on these coefficients to increase compression ratio significantly. VQ algorithms are applied on transformed image and codebooks of minimum possible size 16 and 32 are generated.

FouadKheliÞ(2018)[11], This paper is aimeda model for storing and sharing data securely through the cloud has been presented. RDH-EI has been recently suggested as an approach to ensure secure and privacy-preserving applications for data sharing and management in the cloud, limitations have been reported on the efficiency of conducting RDH in such applications. To address security issues in the cloud more efficiently, a new approach that does not use the process of RDH has been proposed. This is based on the idea of reserving room before encryption via a wavelet-based lossless image coder. Compared with state of- the-art RDH-EI systems, the proposed approach has been shown to offer a significantly higher data insertion capacity with suitable features for the presented cloud model.

RanjeetKumar(2019)[12], The present paper makesan efficient compression and quality retrieval technique is presented for high resolution or big data images based on low-rank singular value analysis. The proposed technique has been able to compress the image at higher compression rate with acceptable visual quality as per human vision system (HVS), the comparative analysis also considers as evidence that explain the suitability of proposed method as compare to state-of-the techniques and standard technique like JPEG200.

MamtaMeena(2016)[13],This paper deals with the newly proposed architecture on cloud can resolved many issues of legacy system. Standalone system has many drawbacks, to full fill today requirements which can be overcome using cloud. By using this we can see how the images will be uploaded, and how they will be stored in a blob storage on cloud. The public cloud based model using CBIR SaaS Architecture presented in this paper has been successfully implemented by Microsoft Azure. This system can be easily scalable, pluggable and more effective in terms of cost & efficiency. Because of its flexible on-demand principle, it can operate enormous amount of data, which in turn, gives effective use of data storage and processing power. We are going to propose a highly scalable, pluggable and faster cloud based CBIR system, which is capable to store, process and extract and operate large number of images. System can be scalable based on the storage and processing requirements.

B. Nivedha(2017)[14], The author of this paper investigateImage redundancy in the feature, spatial, and frequency domains. We first organize the

images into a pseudo video by minimizing the global prediction cost in the feature domain. A hybrid disparity compensation method to better exploit both the global and local correlations among the images in the spatial domain. The redundancy between each compensated signal and the corresponding target image is adaptively reduced in the frequency domain.

J. Smith(2012)[15], The present paper examines a progressive encoding technique that encodes the structure as well as the plane equations. We encode the planes using distances to three points and a single bit. To decode these planes, we solve a constrained optimization problem that has closed-form solution. We then reconstruct the surface from this representation by implicit zing the discontinuous linear pieces at the leaves of the octree and take a level set of this implicit representation. Our tests show that the proposed method compresses surfaces with higher accuracy and smaller file sizes than other methods. To acquire these models, one typically uses a laser range scanner that generates 3D point samples on the surface of the object.

3. PROPOSED METHODOLOGY

3.1 Model Details

Cloud computing is a modern technology which is growing rapidly throughout the world. The users make use of cloud storage to save the data on cloud and that can be accessed from anywhere and anytime. But at the same time, user is mostly concerned about the validation of data which stored in the cloud. Therefore, to check the validation of data (auditing), an entity called Third Party Auditor (TPA) is used. There are various privacy preserving data auditing schemes which have their own benefits and limitations. Therefore, there is a need to develop auditing scheme which overcomes all these limitations of existing approaches. A new privacy preserving and dynamic public audit service for secure cloud storage is proposed which is secure and efficient to use. It consists of three key units: data owner, TPA, and cloud server. Data owner does several actions as piercing a file into blocks, encoding it, producing a hash value for each block, merging it, creating a signature on it and does dynamic data processes such as adding, modifying, deletion of data. TPA does validation of data while performing various activities such as producing hash value for encrypted blocks which is acknowledged from cloud server, merged them then generating new signature on this. After words, it matches both the signatures to check the correctness of information. Validation of data done either periodically or on user's demand. Cloud server saves the encoded blocks of file. The main objective is to develop an audit service which holds the abilities as privacy preserving, public auditing, and data integrity along with privacy.Propose a new approach in the challenge of data ownership and cryptography to manage the storage of encrypted data with Data Auditing. We are motivated to save data in the cloud and to preserve the privacy of data owners by proposing a scheme to manage the storage of encrypted data with auditing. We test safety and evaluate the performance of the proposed scheme through analysis and simulation. The results show its efficiency, effectiveness and applicability.

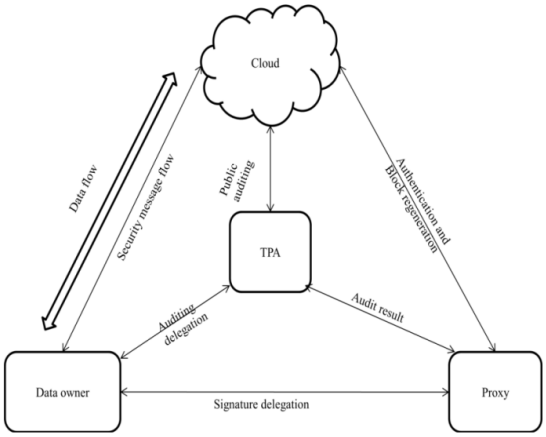

Figure 3.1: Proposed System Architecture

MODULES:

1. System Model
2. Construction of Our Auditing Scheme
3. Mitigating the Overhead of Data Owner
4. Enabling Privacy-Preserving Auditable

MODULES DESCSRIPTION:

1. System Model

We consider the auditing system model for Regenerating-Code-based cloud storage, which involves four entities: *the data owner*, who owns large amounts of data files to be stored in the cloud; *the cloud*, which are managed by the cloud service provider, provide storage service and have significant computational resources; *the third party auditor* (TPA), who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers; and *a proxy agent*, who is semi-trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers

during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may becomes off-line even after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy.

2. Construction of Our Auditing Scheme

Our auditing scheme consists of three procedures: Setup, Audit and Repair. To correctly and efficiently verify the integrity of data and keep the stored file available for cloud storage, our proposed auditing scheme should achieve the following properties: Public Auditability: To allow TPA to verify the intactness of the data in the cloud on demand without introducing additional online burden to the data owner. Storage Soundness: To ensure that the cloud server can never pass the auditing procedure except when it indeed manage the owner's data intact. Privacy Preserving: To ensure that neither the auditor nor the proxy can derive users' data content from the auditing and reparation process. Authenticator Regeneration: The authenticator of the repaired blocks can be correctly regenerated in the absence of the data owner. Error Location: To ensure that the wrong server can be quickly indicated when data corruption is detected.

3. Mitigating the Overhead of Data Owner

Despite that the data owner has been released from online burden for auditing and repairing, it still makes sense to reduce its computation overhead in the Setup phase because data owners usually maintain very limited computational and memory resources. As previously described, authenticators are generated in a new method which can reduce the computational complexity of the owner to some extent; however, there exists a much more efficient method to introduce further reduction. Considering that there are so many modular exponent arithmetic operations during the authenticator generation, the data owner can securely delegate part of its computing task to the proxy in the following way: The data owner first properly augments the m native blocks, signs for them, and thus obtains and, then it sends the augmented native blocks and to the proxy. After receiving from the data owner, the proxy implements the last two steps of *SigAndBlockGen(·)* and finally generates entire authenticators for each segment with secret value x. In this way, the data owner can migrate the expensive encoding and authenticator generation task to the proxy while itself maintaining only the first two lightweight steps; thus, the workload of data owner can be greatly mitigated.

4. Enabling Privacy-Preserving Auditable

The privacy protection of the owner's data can be easily achieved through integrating with the random proof blind technique or other technique. However, all these privacy-preservation methods introduce additional computation overhead to the auditor, who usually needs to audit for many clouds and a large number of data owners; thus, this could possibly make it create a performance bottleneck. Therefore, we prefer to present a novel method, which is more light-weight, to mitigate private data leakage to the auditor. Notice that in regenerating-code-based cloud storage, data blocks stored at servers are coded as linear combinations of the original blocks with random coefficients. Supposing that the curious TPA has recovered m coded blocks by elaborately performing *Challenge-Response* procedures and solving systems of linear equations, the TPA still requies to solve another group of m linearly independent equations to derive the m native blocks. We can utilize a keyed pseudorandom function to mask the coding coefficients and thus prevent the TPA from correctly obtaining the original data. Specifically, the data owner maintains a secret key in the beginning of the Setup procedure and augments m original data blocks.

3.2 Algorithm details

3.2.1 AES with Key generation Phase:

AES with SHA Key: For encrypting metadata file we are using AES encryption algorithm. The encryption process generates a symmetric key called around a key. SHA-1 is applied on this key which creates block of data which is hold by an array of data called the state array. The method can create 128/192/256-bit keys.

Algorithm: Keypair generation algorithm

Data :userKey

Result : SecretKeySpec*secreteKey*

```
1 byte[] key= userKey.getBytes("UTF-8");
2 MessageDigestsha = MessageDigest.getInstance("SHA-1");
3 key = sha.digest(key);
4 key = Arrays.copyOf(key, 16);
5 SecretKeySpecsecretKey = new SecretKeySpec(key,"AES");
return secreteKey;
```

The process is using AES for metadata file encryption because AES is faster than Triple DES, AES is stronger than the Triple-DES. , AES is easy to implement in any higher-level language

3.2.2 Metadata File Encryption:

Algorithm: Metadata file encryption

Data: File *F*, SecretKey*secret key*

Result: Ciphertext*CT*

```
1 setKey(secreteKey);
2Cipher Transform Secure Cipher = Cipher Transform.getInstance("AES/ECB/PKCS5Padding" );
3 SecureCipher.init (CipherTransform.ENCRYPT_MODE, secreteKey);
4 CT Base64.getEncoder().encodeToString (SecureCipher.doFinal(F.getBytes("UTF-8")))
5 return CT
```

3.2.3 Decryption:

In Method follows a process which is before reconstructing the image file joiner needs the sequence of chunks in which they are being joined. This sequence information is stored in a metadata file which is being encrypted before storing it in the cloud. So the decryption module decrypts the metadata file for file joiner

Algorithm: Metadata file decryption

Data: Ciphertext*CT*, Cipher key *CK*

Result: File *F*

```
1 setKey(CK);
2CipherTransform Secure Cipher = CipherTransform.getInstance ("AES/ECB/PKCS5Padding");
3 SecureCipher.init (CipherTransform.DECRYPT_MODE, CK);
4 F = SecureCipher.doFinal (Base64.getDecoder().decode(CT)
5 return F
```

3.2.4 TPA Process:

The system has three main models which are involved. Cloud users, cloud storage and third-party auditor are the part of it. Cloud storage and cloud service provider are the same in this system. Cloud users stored the data over the cloud by registering to a particular cloud storage provider. Data owner's stored' data on cloud storage space. The public cloud service provider is only responsible for storing data and is not responsible for any damage of data to give a proof of the integrity of the stored user's data. The system uses TPA for the process of auditing. TPA is nothingbut an analyzer which verifies the data integrity on behalf of users in the system and minimizes the overload of the user. To have successful TPA Following security and performance challenges should be achieved

1) Efficiency: While data uploading and auditing of data, data transfer, communication and computation cost must be low.

2) Storage accuracy: TPA should complete the auditing task and pass it without data on that side or damaging stored data.

3) Privacy-preserving: TPA should not exploit data of users while collecting for the process of auditing. 4) Prohibit Attacks: -To ensure that the frame and collude attack should not take place

Algorithm: Data verification

Data: File *F*, Public key *PuK*,
Users Digital Signature *UDigSign*

Result: Verified result *R*

```
1 Signature dSign
 = Signature.getInstance(MD5withRSA);
2 dSig.initVerify(PuK);
3 dSig.update(F.getBytes());
4 R=dSig.verify(UDigSign);
5 returnR;
```

3.2.5 FRAGMENTATION ALGORITHM

Input: File

Output: Chunks

Step1: If file is to be split go to step 2 else merge the fragments of the file and go to step

Step2: Input source path, destination path
Step3: Size = size of source file
Step4:Fs = Fragment Size
Step5:NoF = number of fragments
Step6:Fs = Size/Nof
Step7: We get fragments with merge option
Step8: End

3.2.6 MD5 (Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Steps:

1. A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
2. The output of a message digest is considered as a digital signature of the input data.
3. MD5 is a message digest algorithm producing 128 bits of data.
4. It uses constants derived to trigonometric Sine function.
5. It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
6. Most modern programming languages provides MD5 algorithm as built-in functions

4. RESULTS AND DISCUSSION

4.1 Results 1: Show File Size and Encryption Time

In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel processor 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as AES (Proposed system), CP-ABE (Existing System).

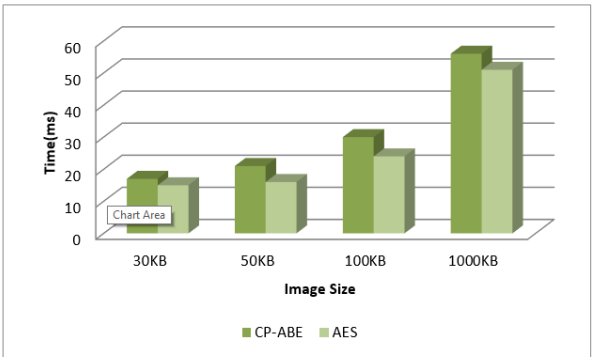

Figure 4.1: Shows file size on x axis and Encryption Time on Y-axis

Table 4.1: Show File Size and Encryption Time

Index Number	Image size (KB)	CP-ABE Encryption Time	AES Encryption Time
1	30	31	28
2	50	36	31
3	100	63	58
4	1000	102	93

4.2 Results 2: Show File Size and Decryption Time

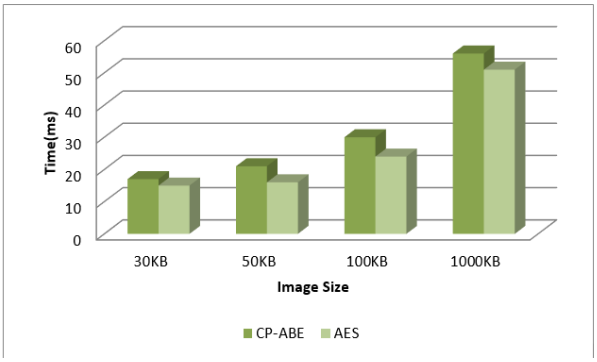

Figure 4.2: Shows file size on x axis and Decryption Time on Y-axis

Table 4.2: Show File Size and Decryption Time

Index Number	Image size (KB)	CP-ABE Decryption Time	AES Decryption Time
1	30	12	9
2	50	16	12
3	100	26	21
4	1000	52	46

4.3 Results 3: Show File Size and Uploading Time

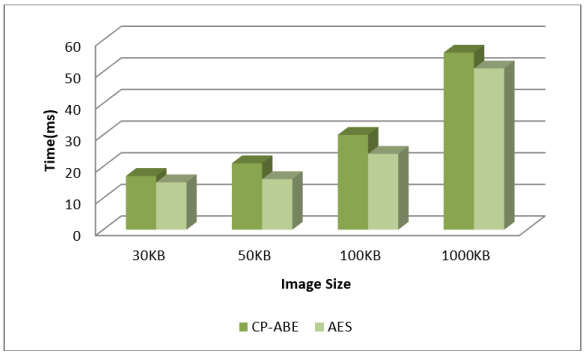

Figure 4.3: Shows file size on x axis and Uploading Time on Y-axis

Table 4.3: Show File Size and Uploading Time

Index Number	Image size (KB)	CP-ABE uploading Time	AES uploading Time
1	30	36	32
2	50	42	35
3	100	69	62
4	1000	111	96

4.4 Results 4: Show File Size and Downloading Time

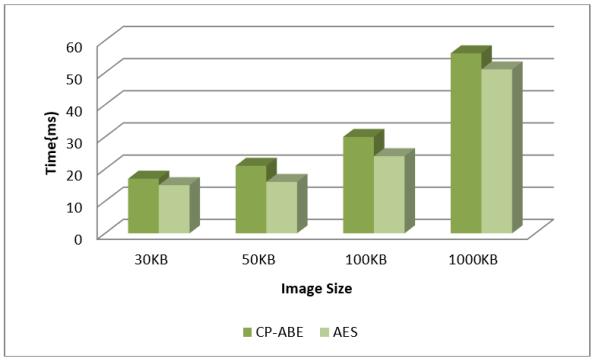

Figure 4.4: Shows file size on x axis and Downloading Time on Y-axis

Table 4.4: Show File Size and Downloading Time

Index Number	Image size (KB)	CP-ABE Downloading Time	AES Downloading Time
1	30	17	15
2	50	21	16
3	100	30	24
4	1000	56	91

6.5 Results 5: overall system execution table

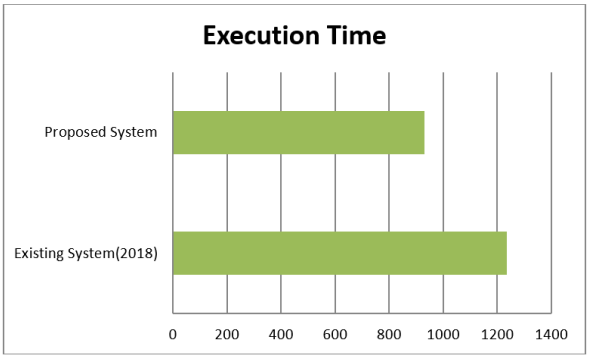

Figure 4.5: overall system execution graph

Table 4.5: overall system execution table

Existing System (2018)	Proposed System
1236	932

4.6 Results 6: Proposed System Image functioning time table

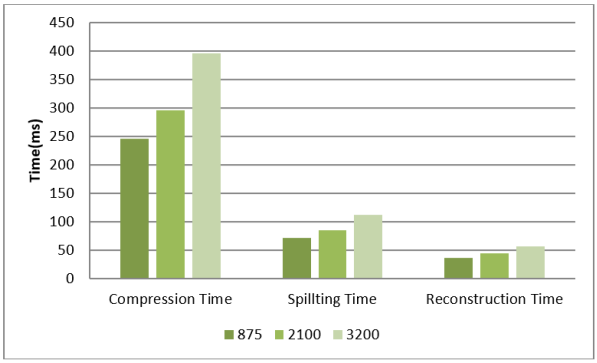

Figure 4.6: Proposed System Image functioning Time graph

Table 4.6: Proposed System Image functioning time table

Image Size (KB)	Image Compression Time	Image Splitting Time	Reconstruction Time
875	245	72	36
2100	296	85	44
3200	395	112	56

Conclusion

Cloud computing is an emerging technology that will receive more attention in the future from industry and academia. To protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage together with data integrity checking and failure reparation becomes

critical. Recently, regenerating codes have gained popularity due to their lower repair bandwidth while providing fault tolerance. Existing remote checking methods for regenerating-coded data only provide private auditing, requiring data owners to always stay online and handle auditing, as well as repairing, which is sometimes impractical. In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage. To solve the regeneration problem of failed authenticators in the absence of data owners, we introduce a proxy, which is privileged to regenerate the authenticators, into the traditional public auditing system model. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating-code-based cloud storage. The cost of this technology is more attractive when it is compared to building the infrastructure. However, there are many security issues coming with this technology as happens when every technology matures. In this research paper data security, data integrity and access control in the public cloud is achieved with significant results. In this process, Third Party Auditor (TPA) and user separation are used successfully. The TPA has a hybrid algorithm for signature generation called MD5withRSA. A new secure and privacy preserving public auditing service is proposed. Privacy preserving public auditing is accomplished with the help of TPA. TPA performs auditing without retrieving the data, therefore preserving the privacy of the data. In this scheme, the data are split into multiple blocks and then stored in the encrypted format at cloud server for storage, thus the secrecy of data is maintained. The modification of data is verified by TPA on request of the data owner by comparing both the signatures, one which is produced by data owner and the other generated by TPA. It only verifies whether the stored data is altered or not and notifies the result to the data owner. The access control is used for separate users from data owners and only those users can have access to the owner's data who have granted access by data owners. Data is compressed without affecting the quality of data to reduce the storage cost. The compressed data is then stored in chunks to provide security. The proposed system can be further extended to improve the TPA performance of different types of data on cloud environment.

REFERENCES

1. Noshina Tariq(2019)[71], The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, Sensors 2019, 19, 1788; doi:10.3390/s19081788 www.mdpi.com/journal/sensors
2. Xin Dong(2014)[72], Achieving an effective, scalable and privacy-preserving data sharing servicein cloud computing, *computers & s e c u rity* 4 2 (2 0 1 4) 1 5 1 e1 6 4 , journal homepage: www.elsevier.com/locate/cose Available online at www.sciencedirect.com
3. Yunchuan Sun(2014)[73], Data Security and Privacy in Cloud Computing,*Hindawi Publishing Corporation International Journal of Distributed Sensor Networks* Volume 2014, Article ID 190903, 9 pageshttp://dx.doi.org/10.1155/2014/190903
4. L. Malina(2015)[74], Privacy-preserving security solution for cloud services, Journal of Applied Research and Technology, Vol.13,February 2015
5. Lo'ai A. Tawalbeh(2019)[75], Reconsidering big data security and privacy in cloud and mobile cloud Systems, *Journal of King Saud University – Computer and Information Sciences* journal homepage: www.sciencedirect.comhttps://doi.org/10.1016/j.jksuci.2019.05.007
6. Zhongbo Shi(2014)[6], Photo Album Compression for Cloud Storage Using Local Features, *IEEE Journal On Emerging And Selected Topics In Circuits And Systems*, Vol. 4, No. 1, March 2014 Digital Object Identifier 10.1109/JETCAS.2014.2298291
7. RajkumarBuyya(2013)[7], Introduction to the IEEE Transactions on Cloud Computing, *IEEE Transactions On Cloud Computing*, Vol. 1, No. 1, January-June 2013 2168-7161/13/$31.00 © 2013 IEEE
8. IsranaHossainArka(2014)[8], Collaborative Compressed I-Cloud Medical Image Storage with Decompress Viewer, *International Conference on Robot PRIDE 2013-2014 - Medical and Rehabilitation Robotics and Instrumentation, Conf. PRIDE 2013-2014*, Procedia Computer Science 42 (2014) pp. 114 – 121 Available online at www.sciencedirect.comdoi: 10.1016/j.procs.2014.11.041

9. SajidaKarim(2020)[9], The evaluation video quality in social clouds, *Entertainment Computing* 35 (2020) 100370, journal homepage: www.elsevier.com/locate/entcom, Contents lists available at Science Direct https://doi.org/10.1016/j.entcom.2020.100370
10. H. B. Kekre*(2016)[10]*, Color Image Compression using Vector Quantization and Hybrid Wavelet Transform, *Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016)*,Procedia Computer Science 89 (2016) pp. 778 – 784, Available online at www.sciencedirect.com, doi: 10.1016/j.procs.2016.06.059
11. FouadKheliÞ(2018)[11], Secure and Privacy-preserving Data Sharing in the Cloud based on Lossless Image Coding, *Preprint submitted to Signal Processing February 13, 2018* DOI: 10.1016/j.sigpro.2018.02.016
12. Ranjeet Kumar(2019)[12], An efficient technique for image compression and quality retrieval using matrix completion, *Journal of King Saud University – Computer and Information Sciences* xxx (xxxx) xxx journal homepage: www.sciencedirect.comhttps://doi.org/10.1016/j.jksuci.2019.08.002
13. MamtaMeena(2016)[13], Hybrid Wavelet Based CBIR System using Software as a Service (SaaS) Model on public Cloud, *7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science* 79 (2016) pp. 278 – 286, Available online at www.sciencedirect.comdoi: 10.1016/j.procs.2016.03.036
14. B. Nivedha(2017)[14],Lossless Image Compression In Cloud Computing,*2017 International Conference on Technical Advancements in Computers and Communications,* 978-1-5090-4797-0/17 $31.00 © 2017 IEEE DOI 10.1109/ICTACC.2017.37
15. J. Smith(2012)[15], Progressive encoding and compression of surfaces generated from point cloud data, *Computers & Graphics* 36 (2012) pp. 341–348, Contents lists available at SciVerseScienceDirect journal homepage: www.elsevier.com/locate/caghttp://dx.doi.org/10.1016/j.cag.2012.03.032
16. Man-Wen Tian(2019)[16], Research on image recognition method of bank financing bill based on binary tree decision, *J. Vis. Commun. Image R.* 60 (2019) pp. 123–128 journal homepage: www.elsevier.com/ locate/ jvcihttps://doi.org/10.1016/j.jvcir.2018.12.016
17. A.M. Vengadapurvaja (2017)[17], An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security, *7th International Conference on Advances in Computing & Communications, ICACC-2017, 22- 24 August 2017, Cochin, India* Procedia Computer Science 115 (2017) pp. 643–650 Available online at www.sciencedirect.com 10.1016/j.procs.2017.09.150
18. Chi Yang(2013)[18], A spatiotemporal compression based approach for efficient big data processing on cloud, *Journal of Computer and System Sciences,* DOI: 10.1016/j.jcss.2014.04.022 http://dx.doi.org/10.1016/j.jcss.2014.04.022
19. Chaowei Yang(2016)[19], Utilizing Cloud Computing to address big geospatial data challenges, *Computers, Environment and Urban Systems* xxx (2016) xxx–xxx CEUS-01097; No of Pages 9, journal homepage: www.elsevier.com/locate/ceushttp://dx.doi.org/10.1016/j.compenvurbsys.2016.10.010
20. FarhanIsrak Yen(2019)[20], Efficient Image Compression for Cloud System, *2019 International Conference on Sustainable Technologies for Industry 4.0 (STI), 24-25 December*, 978-1-7281-6099-3/19/$31.00 ©2019 IEEE
21. Xingyue Chen(2017)[21], A Remote Data Integrity Checking Scheme for Big Data Storage, *2017 IEEE Second International Conference on Data Science in Cyberspace*
22. Hui Cao(2018)[22],An Efficient Privacy-Preserving Algorithm based on Randomized Response in IoT-based Smart Grid,*2018 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, ScalableComputing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovations*, 978-1-5386-9380-3/18/$31.00 ©2018 IEEE DOI 10.1109/SmartWorld.2018.00160
23. JianShen(2017)[23], Block Design-based Key Agreement for Group Data Sharing in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing,* DOI 10.1109/TDSC.2017.2725953
24. Fran Casino(2013)[24], On Privacy Preserving Collaborative Filtering: Current Trends, Open Problems and New Issues, *2013 IEEE 10th International Conference on e-Business Engineering* 978-0-7695-5111-1/13 $26.00 © 2013 IEEE DOI 10.1109/ICEBE.2013.37
25. WentingShen(2019)[25], Enabling Identity-Based Integrity Auditing and Data Sharing

With Sensitive Information Hiding for Secure Cloud Storage, *IEEE Transactions On Information Forensics And Security*, Vol. 14, No. 2, February 2019 http://www.ieee.org/publications_standards/publications/rights/index.html Digital Object Identifier 10.1109/TIFS.2018.2850312

26. NureniAyofeAzeez(2017)[26], Security and privacy issues in e-health cloud-based system: A comprehensive content analysis, *Egyptian Informatics Journal* xxx (xxxx) xxx journal homepage: www.sciencedirect.com
27. PratikshaMeshram(2014)[27], A System of Privacy Preserving Public Auditing for Secure Cloud Storage System,*International Journal of Engineering Research & Technology (IJERT)* Vol. 3 Issue 8, August – 2014 ISSN: 2278-0181
28. Geeta C M(2018)[28], Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions, *International Journal of Computer (IJC) (2018) Volume 28, No 1 , pp 8-57,* http://ijcjournal.org/
29. David W. Chadwick(2012)[29], A privacy preserving authorisation system for the cloud, *Journal of Computer and System Sciences* 78 (2012) pp. 1359–1373, www.elsevier.com/locate/jcss doi:10.1016/j.jcss.2011.12.019
30. Lilian Edwards(2015)[30], Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective,*CREATe Working Paper Series*, DOI: 10.5281/zenodo.34501
31. Rajawat, Anand Singh, et al.(2021)[31] "Fusion Protocol for Improving Coverage and Connectivity WSNs." IET Wireless Sensor Systems, vol. 11, no. 4, 16 Mar. 2021, pp. 161–168, 10.1049/wss2.12018.
32. Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N., Ghosh, A. (2022)[32]. Reliability Analysis in Cyber-Physical System Using Deep Learning for Smart Cities Industrial IoT Network Node. In: Piuri, V., Shaw, R.N., Ghosh, A., Islam, R. (eds) AI and IoT for Smart City Applications. Studies in Computational Intelligence, vol 1002. Springer, Singapore. https://doi.org/10.1007/978-981-16-7498-3_10.
33. Kumar, R. and Varshney, G. (2011)[33] Tourism Crisis Evaluation Using Fuzzy Artificial Neural Network. International Journal of Soft Computing and Engineering, 1, 19-22.
34. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278– 4209