DESIGN A MOBILE CLOUDLET- ZESTFUL VITALITY OPTIMIZATION TECHNIQUE USING DAZE COMPMPUTING MODEL

Research Scholar - **JALLA REDDEPPA REDDY**[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- The growth in mobile devices and applications has leveraged the emergence of mobile cloud computing, which allows the access to services at any place and extends mobile computing. Usually, the current mobile network consists of a restricting factor in supporting such access because, from a global perspective, cloud servers are distant from most mobile users, which introduces significant latency and results in considerably delays on applications in mobile devices. In this research author are going to develop Daze Computing Model Based Mobile Cloudlet-Zestful Vitality Optimization which is more efficient as compare to other existing model. On the other hand, Cloudlet is usually on the edge of Mobile Networks and can serve content to mobile users with high availability and high performance. This thesis reviews both the traditional mobile cloud computing and the Cloudlet architecture. Taxonomy on the Cloudlet architecture is introduced and three related technologies are discussed. Based on the user needs in this environment, personalModel which is used to predict individual behavior and group model which considers caching popular data for several users are proposed. Making use of these two models and the Cloudlet architecture, two data access schemes are designed based on model distribution and data pre-distribution. We have conducted experiments and analysis for both the models and data access schemes. For the models, model efficiency and comparisons among different technologies are analyzed. Simulation results for the data access schemes show that the proposed schemes outperform the existing method from both battery consumption and performance aspects.

Keywords –Cloud Computing, Daze Computing, Mobile Cloudlet, Zestful Vitality Optimization

1. INTRODUCTION

Cloud computing enabled distributed data storage and at the same time reduced the usage costs. Cloud facilitated access to data anytime from anywhere and also from multiple locations. The user is relieved of the complexities of hardware and software needs for data storage and sharing mechanisms and enjoys data -storage location independence. The user can simply utilize the services provided by the different organizations offering cloud services for data storage and access. With ease of access and storage on cloud, the issues of usage authorization and data security pop up. Typically, authorized users, are allowed to access cloud storage with restrictions at different levels, with the access control being managed by the system administrator. One of the restrictions that help securing data is providing access to usage of data for a particular use and to restrict the user's number approaches that can be used for access and usage. Attributes are the deciding factor for some of the user level grouping formation. Content storage and content sharing for different purposes being the major use of cloud, data security while transferring or storing the file is an area of concern requiring efficient solutions.

1.1 Background

In the work the method proposed for privacy-preserving for public data. The data is shared across all users of that cloud the method known as the Oruta method. The public verifier has no right to detect who is the signer on each block yet method can perform the auditing function without all attributes. In the system, the author has used a ring signature for the creation of a homomorphic authenticator on the cloud. The system can perform the batch auditing process on data for fast processing. The authors mentioned two problems that they will study in the future; the first one is traceability that is the original user can reveal the identity in some special situations. The method also supports the data freshness on the cloud while processing a different request from different users. It helps to preserve data identity throw-out the complete process which helps to achieve privacy.

1.2 Motivation

Even though MCC enables enhancement on mobile devices, it massively relies on the mobile network for retrieving data from cloud servers. Besides being restricted by coverage and access, this substantial dependency imposes a considerable burden on the network through constant communication. In the MCC, the cloud is formed by countless data centers which include servers with comprehensive computing and storage capabilities [54]. When mobile terminals connect to the server, the amount of data transmission between servers and mobile terminals, as well as servers and servers, is significantly large, which leads. 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.

1.3 Cloud Security for Privacy Preserving

Cloud security involves the procedures and technology that secure cloud computing environments against both external and insider cyber security threats. Cloud computing, which is the delivery of information technology services over the internet, has become a must for businesses and governments seeking to accelerate innovation and collaboration. Cloud security and security management best practices designed to prevent unauthorized access are required to keep data and applications in the cloud secure from current and emerging cyber security threats.

1.3.1 Cloud computing categories

Cloud security differs based on the category of cloud computing being used. There are four main categories of cloud computing:

Public cloud services, operated by a public cloud provider —These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

Private cloud services, operated by a public cloud provider —These services provide a computing environment dedicated to one customer, operated by a third party.

Private cloud services, operated by internal staff —These services are an evolution of the traditional data center, where internal staff operates a virtual environment they control.

Hybrid cloud services — Private and public cloud computing configurations can be combined, hosting workloads and data based on optimizing factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

Here’s a diagram showing common control plane across cloud models:

1.3.2 Segmentation of cloud security responsibilities

Most cloud providers attempt to create a secure cloud for customers. Their business model hinges on preventing breaches and maintaining public and customer trust. Cloud providers can attempt to avoid cloud security issues with the service they provide, but can’t control how customers use the service, what data they add to it, and who has access. Customers can weaken cyber security in cloud with their configuration, sensitive data, and access policies. In each public cloud service type, the cloud provider and cloud customer share different levels of responsibility for security. By service type, these are:

Software-as-a-service (SaaS) — Customers are responsible for securing their data and user access.

Platform-as-a-service (PaaS) — Customers are responsible for securing their data, user access, and applications.

Infrastructure-as-a-service (IaaS) — Customers are responsible for securing their data, user access, applications, operating systems, and virtual network traffic.

Within all types of public cloud services, customers are responsible for securing their data and controlling who can access that data. Data security in cloud computing is fundamental to successfully adopting and gaining the benefits of the cloud. Organizations considering popular SaaS offerings like Microsoft Office 365 or Salesforce need to plan for how they will fulfill their shared responsibility to protect data in the cloud. Those considering IaaS offerings like Amazon Web Services (AWS) or Microsoft Azure need a more comprehensive plan that starts with data, but also covers cloud app security, operating systems, and virtual network traffic—each of which can also introduce potential for data security issues.

1.3.3 Cloud security challenges

Since data in the public cloud is being stored by a third party and accessed over the internet, several challenges arise in the ability to maintain a secure cloud. These are:

Visibility into cloud data —In many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic.

Control over cloud data —In a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable.

Access to cloud data and applications —Users may access cloud applications and data over the internet, making access controls based on the traditional data center network perimeter no longer effective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud provider personnel could bypass your own security controls.

2. REVIEW OF LITERATURE

BoyangWang(2014)[1],This paper is aimed a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work.

Shini.S.G(2012)[2], The present paper examines Medical Imaging and Cloud computing could become the most data and computing intensive activities in future. Cloud is an emerging approach for various medical imaging applications. In this paper we discussed about cloud based medical imaging mechanism and analyzed the various security issues associated with this approach. We examined the current solutions and discussed their limitations. Finally we discussed the future directions for research. Cloud-based medical image sharing platforms are increasingly becoming more prevalent in medicine.

KaipingXue(2018)[3], The present paper makesa combined the cloud-side and data owner-side access control in encrypted cloud storage, which is resistant to DDoS/EDoS attacks and provides resource consumption accounting. Our system supports arbitrary CP-ABE constructions. The construction is secure against malicious data users and a covert cloud provider. We relax the security requirement of the cloud provider to covert adversaries, which is a more practical and relaxed notion than that with semi-honest adversaries.

Cong Wang()[4], This paper deals witha privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

CONG WANG(2013)[5],The author of this paper investigateoutsourced image recovery service from compressed sensing with privacy assurance. OIRS exploits techniques from different domains, and aims to take security, design complexity, and efficiency into consideration from the very beginning of the service flow. With OIRS, data owners can utilize the benefit of compressed sensing to consolidate the sampling and image compression via only linear measurements. Data users, on the other hand, can leverage cloud's abundant resources to outsource the image recovery related `1 optimization computation, without revealing either the received compressed samples, or the content of the recovered underlying image.

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.

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. KFCG and KMCG are faster in execution and beats performance of LBG algorithm. KFCG combined with hybrid wavelet transform gives lowest distortion and acceptable image quality at compression ratio 192.

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. Further, visual quality can be improved with SVT on based quality retrieval process as per required applications.

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.

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. the fast development and prevailing use of handheld cameras, cost as well as required photography skills is much lower than before.

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. These point samples need to be processed further since almost all applications require polygonal models with explicit connectivity. One of the main difficulties that have hampered the performance of surface reconstruction methods in recent years is the sheer quantity of data.

Man-Wen Tian(2019)[16], This study examinesoccurs when both parties conclude the agreement, where one party issues financial paper as the creditor, and the other one party accepts the financial paper as the debtor, the drawer will repay the money to the payee on the expiry date of financial paper for paying off the debt. Financial paper identification system is a hot issue of current file analysis and identification system, including a series of process, such as paper classification, image processing, character segmentation and identification, as well as file image compression. A research on multiple aspects of financial paper identification system was made, and a financial paper identification system with applied value is thereby established on its basis.

A.M. Vengadapurvaja (2017)[17], The main part of this paperThe Fully Homomorphism Encryption scheme supports both addition and multiplication. The input images and the corresponding encrypted images are shown. The DICOM image is taken as the input image. The analysis like key space analysis, Key sensitivity analysis, histogram analysis, correlation analysis, PSNR and MSE analysis, Noise analysis are performed. The results are tabulated. The analysis that is performed helps us to verify the efficiency of the proposed method in medical image security. When compared to the paper records this method has several advantages.

Chi Yang(2013)[18], This study examinesCloud promises an ideal platform with massive computation power and storage capacity for processing big data that is of high variety, volume, veracity, and velocity. To reduce the quantity and the processing time of big data sets encountered by the current typical Cloud big data processing techniques, in this paper, we proposed a spatiotemporal compression based approach on Cloud to deal with big data and big graph data from real world applications. In our technique, the big data was compressed firstly according to its spatiotemporal features on Cloud. Based on this spatiotemporal compression, a data driven scheduling was developed to allocate the computation and storage of Cloud for providing better big data processing services. The evaluation was conducted over our U-Cloud platform to demonstrate that the spatiotemporal compression could significantly reduce the data size compared to the previous big data processing techniques on Cloud.

ChaoweiYang(2016)[19], The main part of this paperinvestigates how Cloud Computing can be utilized to address Big Data challenges to enable such transformation. We introduce and review four geospatial scientific examples, including climate studies, geospatial knowledge mining, and land cover simulation, and dust storm modelling. The method is presented in a tabular framework as a guidance to leverage Cloud Computing for Big Data solutions.

FarhanIsrakYen(2019)[20], This study examines an idea of compressing images using a distributed system to reduce the storage requirement of data (with images). The proposed strategy can provide storage efficiency with an easier way to compress and reconstruct the image in future when needed.An efficient way to compress/decompressimage for cloud applications. The compression strategysimply takes the image from any source and divides it by thepixel size of the image and stores the final key-value pairsusing Hash Map in the Hadoop distributed file system.

3. PROPOSED METHODOLOGY

3.1 Cloudlets

Although centralized cloud computing exhibits abundant resources for computation-intensive tasks, the unpredictable and unstable communication latency between the mobile users and the cloud makes it challenging to handle latency-sensitive mobile computing tasks. To address this issue, cloudlet [97] recently was proposed by pushing the cloud computing to the network edge closer to the users. Cloudlet is first introduced in as a trusted, resource-rich computer or cluster of machines that is well-connected to the Internet and available for use by nearby mobile devices. Later in 2014, paper depicts Cloudlet as a proximate fixed cloud consists of one or several resource-rich, multi-core, Gigabit Ethernet connected computers aiming to augment neighboring mobile devices while minimizing security risks, offloading distance (one-hop migration from mobile to Cloudlet), and communication latency.

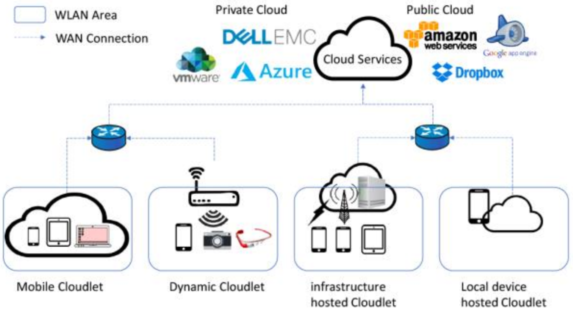


Figure 3.1: The general concept of a Cloudlet

3.2 Model Details

The proposed work has a constructive and flexible data-sharing framework with a third-party auditor in figure 3.1. It supports to maintain the integrity of the user and user's data on cloud while different operations performing in the environment. Our goal is to provide easy data sharing over various cloud storage platform while maintaining data confidentiality. In the proposed work data splitting methodology is used and also a simplified encryption technique .This used to provide data security over cloud data storage. In the work Third Party Auditor (TPA) is used to keep watch on the data process on the cloud. It helps to verify the data on the public cloud.

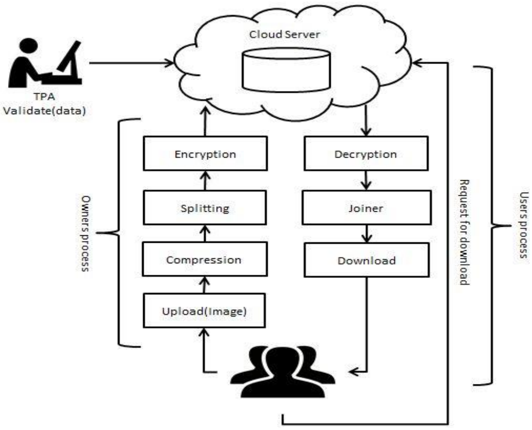


Figure 3.2: Proposed System

MODEL DETAILS

Owners Process:

The data owner owns the data and is likely to share owned data to other users. Data owner stores data over cloud servers which are handled by cloud service providers. In the process of sharing the user processes on it. A data owner first constructs a protocol which contains data access rules for various users, and applies those rules over the data. Then, the owner sends the compressed, split and encrypted data to cloud servers.

Data sampling phase

File Compressor:

File compressor is responsible for taking images as input and compresses them using the DCT algorithm. The process is using DCT because DCT is relatively simple to compute, it is separable (you can do separate DCTs for rows and columns) and has pretty well "energy compaction" properties, Since JPEG, it has been replaced by other transforms which are even simpler and can be computed in fixed-point arithmetic. (Andrew B. Watson (n.d.)). The working can be simply explained as:

Encoded data is written onto a text file with name image.txt {this text file has lesser bytes than original image = Compression}

RLE2image reads image.txt and decodes it into image again, writing a new compressed image onto disk.

Algorithm: File Compression

Data: File I

Result: FilecI

```
1) Lo_D, Hi_D, Lo_R, Hi_R = Haar wavelet transformation (I)
2) vector c = Wavelet Decomposition ( Lo_D, Hi_D )
3) bookkeeping matrix s = Wavelet Decomposition ( Lo_D, Hi_D )
4) Calculate(threshold t, coefficients for compression q)
    5) cI = Compress(c, s, t)
```

File Splitter:

This module is responsible for splitting an image into chunks and store in the cloud, after splitting a file into chunks in creates metadata file. The file contains all associated data with the split file. This file stored on a cloud service provider.

Algorithm: File division into chunks:

Data : File I

Result : File chunks C, metadata ile

```
1 Read(I)
2 file size = fileByteArray.length
3 chunksize = image size / chunknumber
4 foreachsubchunksize in chunksize
5 Write C[i] = subchunksize
6 Store subchunksize in metadata file
```

Security keys generation phase:

Algorithm: Keypair generation algorithm

Data: int key bit size

Result: PrivateKeyprkey, PublicKeypukey

```
AsymmetricKeyPairGenerator generator =
AsymmetricKeyPairGenerator.getInstance(RSA);
SecureRandomNumberGenrandomNumber =
SecureRandomNumberGen.getInstance
("SHA1PRNG","SUN");
randomNumber.setSeed
( System.currentTimeMillisecond());
generator.initialize(keyBitSize, randomAlg);
return generator.generateAsymmetricKeyPair();
```

The digital signature generation phase:

For data verification purpose, in this process it uses MD5 with RSA algorithm. MD5 is a hash function and also it is a cryptographic function that generates a 32-bit message digest for the same. In the proposed method hash value is generated for each value of data uploaded on the cloud, while generating this it uses the MD5 algorithm in the process. This hash value is generated from all attribute values from the user's data. The RSA and Hybrid Algorithm has done investigate with a different attack like brute force, timing, and mathematical.

Algorithm: Digital Signal Generation

Data: File F, PrivateKeyPrK

Result: Digital Signature DigSign

```
Signature dSign =
Signature.getInstance(MD5withRSA)
dSign.initSign(PrK)
dSign.update(F.getBytes())
DigSign = dSign.sign()
returnDigSign
```

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 : SecretKeySpecsecreteKey

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

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

Table 3.1. Comparative analysis between cryptographic algorithms

Parameters	DES	Triple DES	AES
Length of Key in Bits	56	112, 168	128, 192, 256
Number of rounds	16	48	10,12,14
Encryption Speed	Low	Low	Faster than DES and Triple DES
Security Level	Ample security	Ample security	Excellent Security
Effectiveness	Slow in software and also with hardware process	The algorithm is slower in the software	Efficient in the use of software and hardware.

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
```

USERS PROCESS

File Joiner:

File Joiner is responsible to reconstruct the image from split chunks which are stored overcloud. In a process before sending the requested image to the user file joiner gets the location of splitter chunks and joining is done with the use of metadata file content. It joins the chunks and reconstructs an image.

Algorithm: File division into chunks

Data : File chunks IC[ ]

Output : File I

```
1 foreach chunk in file chunk
2 fileByteArray = Read(IC[index])
3 I.append(fileByteArray)
4 Write I
5 End
6 return I
```

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
```

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,

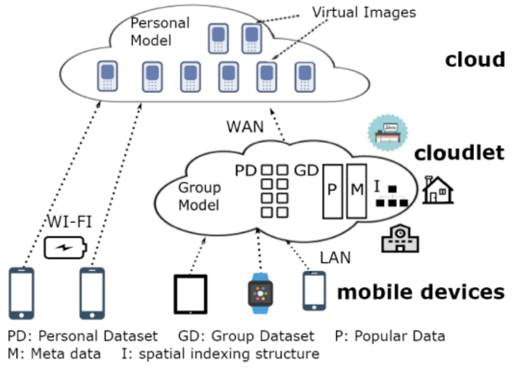
Users Digital Signature UDigSign

Result: Verified result R

Algorithm: Association rules generation algorithm

```
Input: frequent itemsets F
Output: association rules R
R = ;; I = ;
//generate _rst kind rule
for every itemsetlj in F1 do
    I = I [ lj[1]
    if support(lj[1]) _ minconf then
        R = R [ f0) lj[1]0g
    end
end
//generate second kind rule
k = j F j
while Fk 6= ; and I 6= ; do
    for each itemset li in Fk do
        for each dataitem li[j] in itemset li do
            if li[j] 2 I and support(li)
            support(li[j]) _ minconf then
                R = R [ 0li[j] ) fli / li[j]g0
                I = I / li[j]
            end
        end
    end
    return k
end
```

3.2 Proposed Architecture



Personal Model
Virtual Images
cloud
WAN
cloudlet
PD
GD
Group Model
P
M
I
WI-FI
LAN
mobile devices
PD: Personal Dataset GD: Group Dataset P: Popular Data
M: Meta data I: spatial indexing structure

Figure 3.2: a proposed framework

Figure 3.2 demonstrates the overall framework of the proposed architecture. The framework contains four main models. The security model is responsible for generating key pair and digital signature for the user and the owner model uses the RSA algorithm for key pair generation and MD5 with RSA algorithm for digital signature generation.

Conclusion

In this research author are work on the growth in mobile devices and applications has leveraged the emergence of mobile cloud computing, which allows the access to services at any place and extends mobile computing. Usually, the current mobile network consists of a restricting factor in supporting such access because, from a global perspective, cloud servers are distant from most mobile users, which introduces significant latency and results in considerably delays on applications in mobile devices. In this research author are going to develop Daze Computing Model Based Mobile Cloudlet- Zestful Vitality Optimization which is more efficient as compare to other existing model. On the other hand, Cloudlet is usually on the edge of Mobile Networks and can serve content to mobile users with high availability and high performance. This thesis reviews both the traditional mobile cloud computing and the Cloudlet architecture. Taxonomy on the Cloudlet architecture is introduced and three related technologies are discussed. Based on the user needs in this environment, personal Model which is used to predict individual behavior and group model which considers caching popular data for several users are proposed. Making use of these two models and the Cloudlet architecture, two data access schemes are designed based on model distribution and data pre-distribution. We have conducted experiments and analysis for both the models and data access schemes. For the models, model efficiency and comparisons among different technologies are analyzed. Simulation results for the data access schemes show that the proposed schemes outperform the existing method from both battery consumption and performance aspects.In this process, Third Party Auditor (TPA) and user separation are used successfully. The TPA has a hybrid algorithm for signature generation called MD5withRSA. 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. Boyang Wang(2014)[1], Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, IEEE Transactions On Cloud Computing, Vol. 2, No. 1, January-March 2014, pp. 43-56
2. Shini.S.G(2012)[2], Cloud Based Medical Image Exchange-Security Challenges,Procedia Engineering 38 (2012) pp. 3454 – 3461, Available online at www.sciencedirect.comdoi: 10.1016/j.proeng.2012.06.399
3. KaipingXue(2018)[3], Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage, IEEE Transactions on Information Forensics and Security http://www.ieee.org/publications_standards/publications/rights/index.html, DOI 10.1109/TIFS.2018.2809679,
4. Cong Wang()[4], Privacy-Preserving Public Auditing for Secure Cloud Storage,
5. CONG WANG(2013)[5], Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud, IEEE Transactions On Emerging Topics In Computing, Volume 1, No. 1, June 2013 , pp. 166-177 Digital Object Identifier 10.1109/TETC.2013.2273797
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. Rajawat, A.S., Rawat, R., Shaw, R.N., Ghosh, A. (2021)[23]. Cyber Physical System Fraud Analysis by Mobile Robot. In: Bianchini, M., Simic, M., Ghosh, A., Shaw, R.N. (eds) Machine Learning for Robotics Applications. Studies in Computational Intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_4
24. 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
25. 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
26. 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
27. Srivastava, S., Kumar, R.: (2013)[27] Indirect method to measure software quality using CK-OO suite. International Conference on Intelligent Systems and Signal Processing (ISSP), Gujarat, pp. 47–51 (2013)