The International Journal Of Engineering And Science (IJES)
||Volume||2 ||Issue|| 4 ||Pages|| 09-17 ||2013||
ISSN(e): 2319 – 1813 ISSN(p)**:** 2319 – 1805

A Modified Fast Accessing Security Mechanism Using Merkle Hash Torrent Extention for Cloud Computing Environment

R.Ushadevi[1] And V. Rajamani[2]
[1]*Research Scholar, Department of Computer Applications, St. Peter's University, Chennai Tamilnadu, India*
[2]*Department of Electronics and Communication Engg. ,Indra Ganesan College of Engg, Manikandam, Tiruchirappalli,*

----------Abstract----------
A modified fast accessing security mechanism using Merkle torrent extention for cloud computing environment is presented in this paper. Cloud computing mechanism transfers the data to third party auditor using private key and public key. It cannot transfer the large size data cloud and it using the security service provides the user to transfer the data from the third party auditor. In this problem overcome using the Merkle Hash and TPA data coloring and watermarking Techniques used to transfer the data cloud. The load image from the server provides the security and stored files from the particular cloud server. TPA sends to the public key from the client and connects to the server. They data provide secret key and those data to be stored in the cloud server, and connect TPA and accept private key and request the user viewing the information from authentication persons, as well as them to be changed or modify in the data cloud server. TPA cannot change data cloud computing mechanism, as well as those data should be stored in the private cloud. The Merkle hash function using the large size data to be transferred in the cloud server mechanism.

Keywords: *TPA, Data Coloring, Merkle Hash, Public key, Private Key, Cloud computing mechanism*

Date of Submission: 20 March 2013 Date of Publication: 15April 2013

I. INTRODUCTION

The Transport Security mechanism [1] protects your application during transport using SSL for authentication and confidentiality. Transport-layer security is provided [2] by the transports mechanisms used to transmit information over the wire between clients and providers, thus transport-layer security relies on secure **HTTP** transport **(HTTPS)** using **Secure Sockets Layer (SSL).** Transport security is a point-to-point security mechanism that can be used for authentication, message integrity, and confidentiality. When running over an SSL-protected session, the server and client can authenticate one another and negotiate an encryption algorithm and cryptographic keys [3] before the application protocol transmits or receives its first byte of data. Security is "live" from the time it leaves the consumer until it arrives at the provider, or vice versa. The problem is that it is not protected once it gets to its destination. For protection of data after it reaches its destination, use one of the security mechanisms that use SSL and also secure data at the message level [4].

Digital certificates are necessary when running secure HTTP transport (HTTPS) using **Secure Sockets Layer (SSL).** The HTTPS service of most web servers will not run unless a digital certificate has been installed. Digital certificates have already been created for Glassfish, and the default certificates are sufficient for running this mechanism, and are required when using Atomic Transactions. However, the message security mechanisms require a newer version of certificates than is available with Glassfish. You can download valid key store and trust store files for the client and server as described in Updating Glassfish Certificates.

In order to protect data in the cloud, the data can be encrypted before being stored in the cloud. Conversely, data being returned from the cloud will be decrypted. Glenn Brunette, an engineer at Sun Microsystems is working on a project called the *cloud safety box [5]***.** The goal of this project is to create an Interface to a cloud storage provider that enables encryption/decryption of content stored in the cloud. An information-centric approach to storing data in the cloud is a self-protection scheme. Data is encrypted and packaged with *a usage policy*. When the data is accessed [5], the data item should only reveal itself to a trustworthy caller based upon the policy. The High Assurance Remote [6] Server Attestation method provides a mechanism for the data owner to *audit how the data is being used*. This can be done to ensure that data is not being abused or leaked. This method does not actually protect the data, but it provides a mechanism [7] for ensuring that security has not been breached.

The Privacy-Enhanced [8] Business Intelligence method encrypts all data stored in the cloud. This is similar to the Encrypting Data method described, however, special features have been added that *allow the data to be searched.* This search ability allows a search query to be encoded, in which case the cloud can then decide if the stored data matches the encoded search query [9]. One option for retaining control of the data is to store it outside of the cloud [10], in an on-site data center. *T*he primary drawback of this approach lies in accessing data from the cloud-based web application.

II. RELATED WORKS

Security means the data transfer between sources to destination. We provide that data before transfer security key after that data can be send. The data cannot open the third party mechanisms [11]-[12]. We use several layers of proven security technologies and processes to provide you with secure online access to your accounts and information. These are continuously evaluated and updated by our experts to ensure that we protect you and your information. These include:

[1] Secure Socket Layer (SSL) Encryption
[2] Authentication
[3] Data Integrity
[4] Ensuring Your Online Safety

2.1 Secure Socket Layer (SSL) Encryption

When you successfully login to online banking or another secure **RBC** website using an authentic user ID and password, our web servers will establish a secure socket layer **(**SSL**)** connection with your computer [13]-[14]. This allows you to communicate with us privately and prevents other computers from seeing anything that you are transacting so you can conduct online business with us safely. SSL provides 128-bit encrypted security so that sensitive information sent over the Internet during online transactions remains confidential.

2.2 Authentication

To protect our users, we provide secure private websites for any business that users conduct with us. Users login to these sites using a valid client number or username and a password. Users are required to create [15] their own passwords, which should be kept strictly confidential so that no one else can login to their accounts.

2.2 Data Integrity

The information you send to one of our secure private websites is automatically verified to ensure it is not altered during information transfers. Our systems detect if data was added or deleted after you send information. If any tampering has occurred, the connection is dropped and the invalid information transfer is not processed

III. ENSURING YOUR ONLINE SAFETY

Find out how these security [16] mechanisms safeguard our communications with you and learn how RBC helps to protect you against fraud. We strongly encourage paper companies to assign third-party auditors [17] To verify their ratings, and paper buyers to give preference to audited paper products. Paper merchants and other distributors are always required for an independent third-party auditing [18]. Purchasing decisions have major economic consequences and must therefore be based on high quality, reliable information. Therefore WWF (World Wide Found) recommends that the data is third-party audited for papers that are published on Check Your Paper, and that auditing is carried out by a nationally or internationally accredited auditor. This will ensure credibility of the rates and reassure buyers who visit the site for information and guidance.WWF does not directly audit or verify the accuracy of the ratings. However, if any party challenges [19] the accuracy of a rating, we will refer the challenge to the relevant auditor and reserve the right to remove the paper from the website.

IV. PROPOSEDWORK

The existing system used to a security mechanism for cloud computing environment based on private key mechanism presented. Users will know neither the exact location of their data nor the other sources of the data collectively stored with the cloud. The data can find in a cloud ranges from public sources which have minimal security concerns to private data containing which has highly sensitive information.Data coloring and water marking techniques used to protect shared the data object and massively. But in these problem overcome using Merkle hash tree and watermarking techniques efficiently securely proved that set of element undamaged and unaltered. In this algorithm using authentication person only can modify the data cloud mechanism. It using the private key and public key in the cloud computing secure the data transfer the third party auditor can any changes to the data in the cloud computing means the TPA cannot changes in the particular data.

The user can divided in the data TPA and public cloud. When the user can verify the data cloud modify or not the TPA which has the copy and send by the private cloud. The data modify means compare to the copy of the cloud and then sent to the private cloud can modified the data in to the user. The TPA cannot modify the cloud computing from the other user the authentication person only modify the cloud computing mechanism.

4.1 Watermarking Techniques

Water marking is the process of adding the user text at the back of image files. And it's used to shading the text into an image files. And it's mainly used for digital patent administration. Static watermarks are stored in the application complete itself. And have been around for a long time. Markowitz and Cooperman and Davidson and Myhrvold are two techniques of static watermarks. According to Markowitz and Cooperman a static watermark is embedded in an image using one of the many media watermarking algorithms. This image then stored in the static data section of the program. Whereas according to Davidson and Markowitz static code watermark a fingerprint is encoded in the basic block sequence of a program's control flow graphs.

Dynamic watermarking of PDF content rules-based. The PDF Watermark Administration screen provided to define rule sets via the Rules tab. If a given request for a PDF document satisfies one of the pre-defined rules, the template associated with that rule is used to watermark a copy of the content before the copy is returned to the requesting user; only the web layout form will be watermarked, the original PDF file unchanged in its vault location.PHP features a wide array of functions for image handling and manipulation. In today's article, we are going to use those functions to create an image watermarking class. This class will operate on two images: a source image and a watermark. As an optional third parameter our class will also accept an alpha value allowing our watermark to contain alpha transparency.

This should be an enjoyable exercise, but hopefully it will also be one that very useful. For example, let us imagine a scenario where you are hired to create a searchable inventory system for a stock photography website. Obviously you will need to protect your client's photographs offering full quality images only to paying customers. To do this, you could create multiple copies of each image, or you could simply implement a watermarking script like the one we are about to create. This script could then add a watermark to any un purchased images, while leaving those that have been purchased unmarked.

4.2 Modified Merkle Hash tree

The market hash tree used to authentication person only modifies the cloud computing mechanism. The user can transfer the data in to the private cloud and then the divided in to the public key and TPA. The TPA copy of data cloud transfer and stored the data in the private cloud when the data modify ask the public cloud and compare to the copy of the data sent to the private cloud then modify the user.

The Merkle Signature Scheme can only be used to sign a limited number of messages with one public key. The number of possible messages must be a power of two, so that we denote the possible number of messages as **(N** Message length) **N=** 2^n(n bit length **(256)).**The first step of generating the public key to generate the public keys X_i and private keys Y_i of 2^none-time signatures. For each public keyX_i, with **1≤i≤** 2^n**,** a hash value **(**h_i hash tree built**)** h_i**=H (**X_i**)** computed. With these hash values **hi** a hash tree built.

We call a node of the tree $N_{i,j}$where **i** denote the level of the node. The level of a node defined by the distance from the node to a leaf. Hence, a leaf of the tree has level **i=0** and the root has level **i=n.** We number all nodes of one level from the left to the right, so that $a_{i,0}$the leftmost node of level **ì.**

In the Merkle Tree the hash values h_i are the leaves of a binary tree, so that H_i=$N_{0,i}$. Each inner node of the tree is the hash value of the concatenation of its two issues. So $N_{1,0} = H(N_{0,0} \,||\, N_{0,1})$ and$N_{2,0} = H(N_{1,0} \,||\, N_{1,1})$**.**

In this way, a tree with 2^n leaves and $2^{n+1} - 1$nodes is built. The root of the tree $N_{i,0}$ is the public key of the Merkle Signature Scheme

4.3 Embedding Techniques

The technique to obtain the coefficients for the power series expansion (on *s*=0) of voltages ***V*** is quite straightforward, once one realizes that equations (2) can be used to obtain them order after order. Consider the power series expansion for $\mathbf{V}(s) = \sum_{n=0}^{\infty} \mathbf{a[n]s^n}$**(**it calculate for the X_i**)** and

$$\mathbf{1/V}(s) = \sum_{n=0}^{\infty} \mathbf{b[n]s^n}\text{(It calculate for the Yi)} \qquad (1)$$

By substitution into equations (1) and identifying terms at each order in $\boldsymbol{S_n}$**,** one obtains:

$$Sn = \sum_k Y_i ak[n] + Y_i^{sn} a_i[\mathrm{n}] = S_i^{*} B_i^{*} \qquad (2)$$

It then straightforward to solve the sequence of linear systems (2) compared original data and user data successively order after order, starting from ***n*=0**. Note that the coefficients of the expansions for ***V*** and ***1/V*** are related by the simple convolution formulas derived from the following identity:

$$\mathbf{N= } V(S)V^{-1}(\mathrm{S})$$

$$V = (\sum_{n=0\ an}^{\infty} \mathbf{s}^n)(\sum_{n=0\ bn}^{\infty} \mathbf{s}^n)$$

$$1/V = a_0\ b_0 + (\sum_{k=0\ a1-k}^{\infty 1} \mathbf{b})$$

$$(\sum_{k=0\ b2-k}^{2} \mathbf{b^k})\,\mathbf{s2} + \ldots + (\sum_{k=0\ an-k}^{\mathrm{n}} {}^{1}) \qquad (3)$$

So that the right-hand side in (2) can always be calculated from the solution of the system at the previous order. Note also how the procedure works by solving just linear systems, in which the matrix remains Constant $\mathbf{N= } V(S)V^{-1}(\mathrm{S})$ compare the $\boldsymbol{X_i}$**,** $\boldsymbol{Y_i}$ already stored and user data compare and then any change or

modify the data in the authenticate persons otherwise cannot changed inTPA. **K** means User data Stored in the TPA database easy to compare the original data in the TPA.

Algorithm 1. Data Coloring and Watermarking Techniques

Step1: In this algorithm is used generic the watermark v with shared the secret key.

Step2: Each pixel size is i.

Step3: Calculate the secret key v(s) and receiving the image 1/v(s) according to equation 1.

Step4: Extract the watermarking $\sum_k Y_i ak[n] + Y_i^{sn} a_i[\mathrm{n}]$ according to equation 2.

Step5: The image data coloring N= $V(S)V^{-1}(\mathrm{S})$ issued to calculate the data coloring and detecting the

coloring according the equation3.

Step 6: Then calculate the difference between the watermarking

$(\sum_{n=0\ an}^{\infty} \mathbf{s}^n)(\sum_{n=0\ an}^{\infty} \mathbf{s}^n)$ It using compare the data and extraction data cloud is contains

$$= a_0\ b_0 + (\sum_{k=0\ a1-k}^{\infty 1} \mathrm{b^k})(\sum_{k=0\ b2-k}^{2} \mathrm{b^k})\quad \mathrm{s2} + \ldots + (\sum_{k=0\ an-k}^{\mathrm{n}} {}^{1})$$

It is used to detection the data coloring and watermarking techniques transfer the image in TPA.

Algorithm 2. Modifying Merkle Hash Function

Step 1: Initialization

1. N: =initialize ->256 bit value of the hash function
2. £: =0->Control Sum
3. a: =0->Message Length

Step 2: Compression functions of for i=1…n-1 following ($|m_i|$>256)

1. N: = f (N,m_i) ->applies hash function
2. a: = a+256 -> Recalculate Message Length
3. £: =£ +m_i ->Calculate Control Sum

Step 3: Compression function

1. a: =a+| mn| ->Calculate the full Message Length in bits
2. m_i: =0^{256}-| mn| ->last Message with zeroes
3. £: =£ + mn -> Update Control Sum
4. N: = f(N, mn) -> Process the last message block
5. H_i:f(N, L) -> Strengthen up by hash message length
6. H_i:f(N, £) ->hash Control Sum

$a_{1,0}$= $H(a_{0,0}||a_{0,1})$the binary difference map between Hand $a_1$with its **i** pixel denoted as a***(i)*** **(H(*i*) ∈ {0,255})** indicating whether H (*i*) and a (*i*) are different. Wherever the watermarked image is manipulated, noises are shown in the corresponding portion of the difference map H. We could also identify what type of manipulation has been done from H. Then the Merkle hash tree function is used to large size data should be transfer the TPA. In the Merkle hash function is used to authorize person only can modify the cloud computing mechanism.$\mathbf{2^{n+1}-1}$The square dependency neighborhood centered at pixel I consisting of $\mathbf{2^n}$pixels including pixel I itself.

The TPA copy of the data stored in the private cloud when the data should be modifying means it compares to the original image files and then copy of the data cloud sent to the private cloud and public cloud.

$$\mathbf{N=}\boldsymbol{V(S)V^{-1}(S)}$$

It compares to the original image files and then modifies the data cloud in the users. It **V(S)** is the original files and **V^{-}1(S)** compare to the data cloud in TPA and then stored in private cloud.

$$\mathbf{V(S)} = \left(\sum_{n=0}^{\infty} an\, \mathbf{s}^n\right)\left(\sum_{n=0}^{\infty} an\, \mathbf{s}^n\right)$$

In the data cloud computing used to embedding detection the data cloud computing using the Merkle hash tree function to compare the step by step to modify the data cloud and stored in the private cloud then compared to the original image files in starting from **n=0**. It compare to the image files then copy of the data cloud stored in the private cloud. In this function used to authorize persons only modify the data cloud and stored in the private cloud.

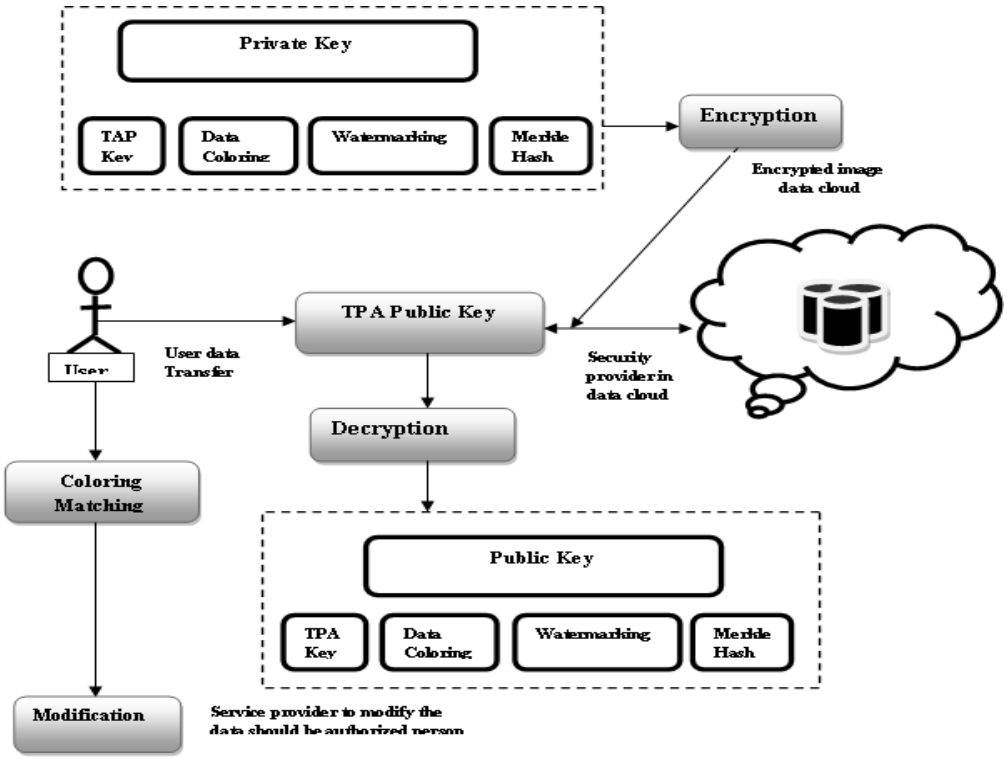
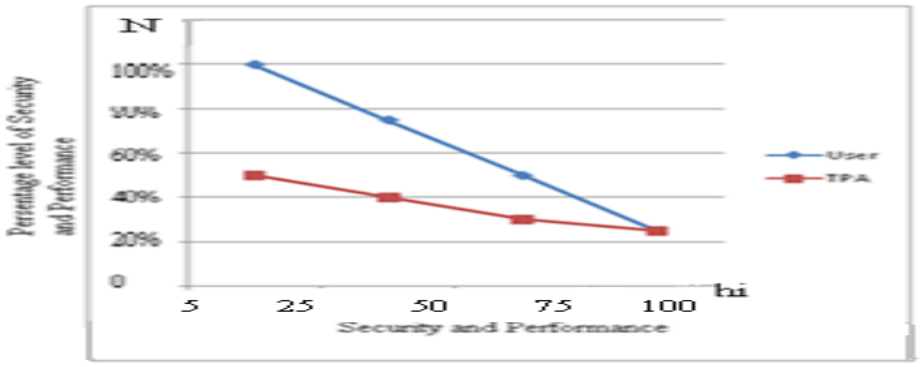


Figure 1 Proposed Architecture

We can use data coloring at unreliable security levels based on the changeable cost function practical. **Figure 1 show** the details involved in the color-matching process, which aims to relate a colored data object with its owner, whose user classification also colored with the same and recognition individuality. The color-matching process guarantees that color applied to user recognition match the data colors. This can initiate various trust-management events, including verification and authorization. Virtual storage supports color generation, embedding, and extraction. Decoloring process should be executed under decryption process. And it followed by Third Party Auditor because **TPA** works to checks user as record or not. Generally, Decoloring the process of reconstruct colored image. And it could be processed during **decryption process**.

V. RESULT AND DISCUSSION

The transactions data cloud computing we compare the security level of our proposed system with the comparison of existing system. Cloud Computing has been envisioned as the next generation architecture of **IT** Enterprise. In this private key used to encrypt for the data to be transferred from the TPA and them should be stored in the database. Those data to be watermarking and data coloring used to transfer the data in the cloud server decrypt the data after that the data will be viewing the authorized persons. The TPA cannot change the data, those authorized persons only can modify and delete for them. In this data to be transferred, provided to the security key after that them to be transferred from another cloud server.



Graph 1. Comparison for Security Level

Figure 2 compares the security level how many data to be transferred in the cloud server based on them stored in the database copy of the data to be transferred in the cloud server? Based on compare to the level them to be transferred in the cloud. The security mechanism cloud computing using the **hi Merkle hash tree** function used to transfer the data between the **TPA** them public cloud and copy of the data stored in the private cloud. The data will be coloring or modification means data should be compare the original files and then modify the authentication persons. Merkle hash function using the large size image file transfer to the cloud computing mechanism. The existing system is used to small size of data should be transferred in this problem overcome used to Merkle hash function to transferred the large size of data should be transferred in particular cloud. User specify for provide the security and then data to be transferred in the cloud server the other persons cannot change in the particular data The TPA data only viewing cannot change the particular data.

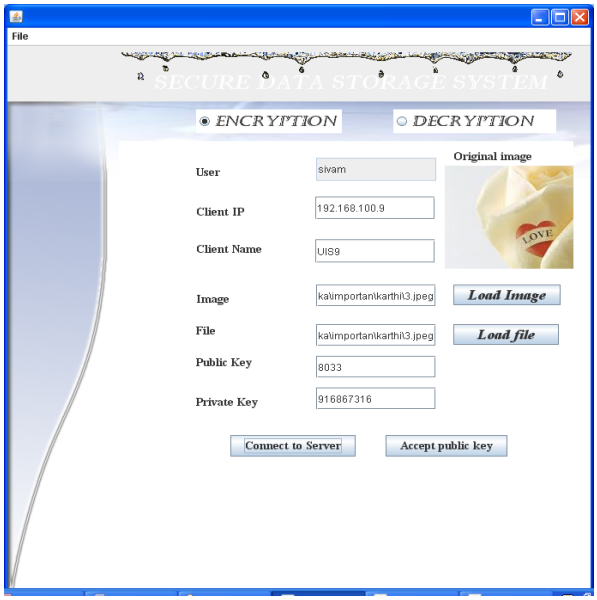


Figure 3 Screen shot of the result - Without Data Coloring and Watermarking Techniques

From Figure 3, we use the original image for data coloring and watermarking process in cloud computing. Without using the data coloring and watermarking techniques data to be transfer the user and TPA. The encrypted the data to be transfer between the user and cloud computing. When the data retrieve from the user encrypted the data and then viewing the details. It use the two method as **Encryption and Decryption method** to security provide in the private key and public key in the cloud computing.

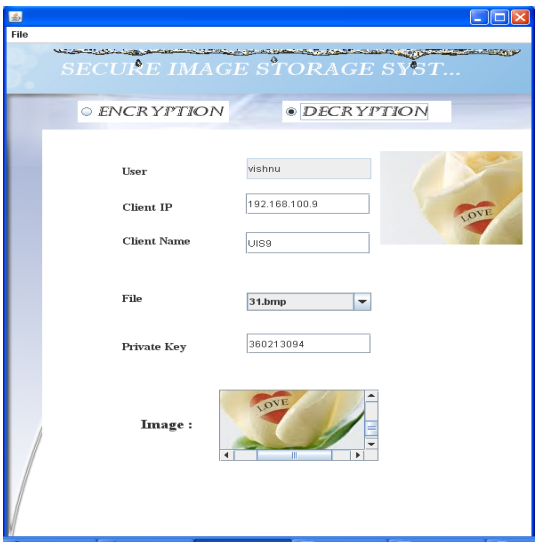


Figure 4 Merkle Hash Function using Cloud Computing Mechanism

In Figure 4**,** we use the Merkle hash function large size data to be transfer between the user and cloud computing mechanism. It provides the security key and then data should be transferred in large size data from the cloud computing mechanism. When the data use from the user compare to the original image and then change the data to authorized persons. The Encrypt and decrypt the data and then the use for the cloud computing mechanism.

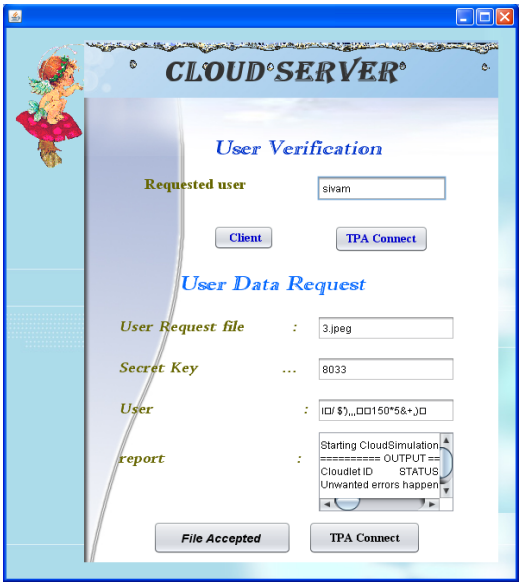


Figure5. Data Stored in the Cloud Server

In Figure 5, we use the data to be stored in the cloud server after the Merkle hash function. The authorized persons only can modify and changes in the cloud computing mechanism. Accept the files and data to be stored in TPA, but cannot change or modify those data, user only can change in the cloud computing mechanism.

VI. CONCLUSION

Data coloring and watermarking techniques used to transfer the data between the user and TPA was presented in this paper using Merkle hash function. It provides the secret key connects to the cloud server transferred data between the user and cloud server. The Merkle hash function using the large size data to be transferred in the cloud server. In this cloud server provides the private key and public key transfer the data from the multi cloud server. The users provide the security key cannot change or modify the TPA the authorized persons only those data should be changed in the cloud computing mechanism.

REFERENCES

[1] G. Divya Zion , D.Kavitha **"**Remote Sensing Data as a Service in HybridClouds: Security Challenges and Trusted ThirdParty Auditing Mechanisms**"**Vol. 1, Issue 7, September 2012.-pg: 1

[2] Sichuan ProvinceEmail: wangshaohui@njupt.edu.cn1. -pg:2

[3] RagibHasan" Securityand Privacyin Cloud Computing**"** Johns Hopkins Universityen.600.412 Spring 2010.-pg:2,5

[4] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S**"** Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud**"** IJCST Vol. 2, Issue 2, June 2011.-pg: 31,34, 61.

[5] EveraldoAguiar**"**An Overview of Issues and Recent Developments in Cloud Computing and Storage Security**"**University of Notre Dame, Notre Dame, IN, e-mail: eaguiar@nd.edu.-*pg: 1, 4,5*

[6] Cong Wang, Qian Wang, and KuiRen**"**Ensuring Data Storage Security in Cloud Computing**"** Email: {cwang, qwang, kren}@ece.iit.edu.-pg:2,3

[7] K.S.Sathiyapriya**"** Integrity And SecurityCheck Through Data Coloring And Water Marking Using Third Party Auditor In Cloud Computing Atmosphere**"**Vol. 2 Issue 1, 2012,95-99.-pg: 1, 2,6.

[8] Nelson Gonzalez1*, Charles Miers1,4, Fernando Red´ıgolo1, Marcos Simplıcio1, Tereza Carvalho1,Mats N¨aslund2 and Makan Pourzandi3 **"**A quantitative analysis of current security concerns and solutions for cloud computing**"**Systems and Applications 2012,-pg:2,3

[9] Wang Shao-huiP 1, 2 *P , Chang Su-qinP1P, Chen Dan-weiP1P, Wang Zhi-weiP **"**Public Auditing for Ensuring Cloud Data Storage Security With Zero Knowledge Privacy**"** 1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing210046, China; pg:1 to 19.

[10] Operations in cloud computing environment**"**vol. 2 no. 10 October 2012.-*pg: 2*

[11] Katukam Ganesh**"** Ensuring and Reliable Storage in Cloud Computing**"** Vol. 3 (5) , 2012,5157 – 5163.pg: 3, 4

[12] D. Kishore Kumar, G.VenkatewaraRao , G.SrinivasaRao**"** Cloud Computing: An Analysis of Its Challenges & Security Issues**"** Issue 5, October 2012.-pg: 1, 2

[13] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S**"** Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud**"** IJCST Vol. 2, Issue 2, June 2011.-pg: 34, 61 and -pg: 31,61

[14] V.KRISHNA REDDY1, L.S.S.REDDY **"**Security Architecture of Cloud Computing**"** Vol. 3 No. 9 September 2011. -pg: 10

[15] Amir Mohamed Talib, RodziahAtan, Rusli Abdullah and MasrahAzrafiAzmiMurad**"**Security Ontology Driven Multi Agent System Architecture for Cloud Data Storage Security: Ontology Development**"** VOL.12 No.5, May 2012.-pg: 1

[16] K.S.Sathiyapriya**"** Integrity And SecurityCheck Through Data Coloring And Water Marking Using Third Party Auditor In Cloud Computing Atmosphere**"**Vol. 2 Issue 1, 2012,95-99.-pg: 1, 6 and -pg:1,2,6

[17] Lee Badger Tim Grance Robert Patt-Corner Jeff Voas**"** DRAFT Cloud Computing Synopsis and Recommendations**"** May 2011.-pg:3

[18] AfsharGanjali**"**Auditing Cloud Administrators Using Information Flow Tracking**"**a.ganjali@utoronto.ca October 15, 2012, pg:2,4

[19] S.S.Karthikkumar**"** An Improved Storage Security Model with Multiple Auditing Task for Cloud Environment**"**Vol. 2 Issue 3, 2012, 18-23.-pg:3.