ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

An Efficient Approach for Security of Cloud Using Watermarking Technique

Navneet Singh[1], SonikaMatele[2], Prof. Shailendra Singh[3]

navneet131088@gmail.com, NITTTR, Bhopal, India [1]

sonikamatele@gmail.com , NITTTR, Bhopal, India [2]

ssingh@nitttrbpl.ac.in, NITTTR, Bhopal, India [3]

Abstract: Cloud computing is the scorching trend now a days. It has many advantages over the other services provided by the dedicated hosting solutions. There are different cloud computing technologies which provide various kind of favourable services. Beside the several benefits of cloud computing, there are lots of issues which need to be adjudicated. One of the most challenging issue is the security. A positive effort has been made in this paper to identify the solution of security issues in cloud computing through combination of digital image watermarking technique and cloud watermarking.

Keywords: Digital Image Watermarking, Apache Hadoop, Discrete Cosine Transform

I. INTRODUCTION

The rapid melioration in the field of cloud computing and with the growth of the virtualizing the environment, it has become necessary to protect the data from various malicious attacks. Since any digital image can be easily copied or modified it is solely the responsibility of the owner of the cloud data center to handle the threats and attacks related to the digital images. Protecting the digital images in the cloud computing environment is the most pivotal issue to be researched on. Whereas the availability and reliability of the digital images is also a major issue to be concerned off. With the digital technology and internet conjecture, all kinds of digital data i.e. images, video, audio frequency are released in network mode, and still there exists some kind of fallibility. So to protect the digital products is to be experimented and implemented on a high priority bases. The intellectual property of a digital image is an important issue at the time when data is moved to and fro amongst various data centers. When classifying broadly the watermarking technology there are two kinds of watermarks, one is the visible watermarking whereas another one is invisible watermarking [4]. The pronominal purpose of visible watermark is to embed a logo on digital image and to claim or promulgate a copyright or ownership of that data. In-spite of some drawbacks of visible watermarks in digital images it is still a strong contender for the securing digital images [1]. The advantages of unseen digital watermark embedding is that it cannot see by naked eyes but not ideal from the perspective for identifying images where the visibility is more important. However a new method was proposed in the year 2007 by C.H chuang known as UVW i.e. unseen visible watermarking in this technique the watermark itself has to be a binary file. These techniques were proposed to augment the robustness of watermark against geometric and non-geometric attack. The watermark is composed not only from a single model but it takes many models such as random digital sequence, digital identification, image and a text model can also be included in this. Now the problems that cloud computing is facing is the problem of data espionage while virtualizing the environment. The location of the data where it is actually stored is unknown to the user so this is also a reason to secure the digital data by watermarking [6]. The watermarking in cloud security are the characteristics negotiated by data owners and service providers.

Taking the scenario of cloud layering system into account to understand its working, three core services are available. The infrastructure as a service is a core or innermost layer that extends to form platform as a service. The platform as a service layer adds operating system and middleware support. Software as a service extends the concept of platform as a service by creating applications on data and metadata with the support of special application programming interfaces. Platform as a service hypostatize infrastructure as a service support and also provides protection at resource management level. This model can also be viewed simply as a service model which states that at software as a service level it provides applications and there management also providing the data and information related to the data or application. Infrastructure as a service requires protection at networking level which is in conjunction with the middleware support that is provided by platform as a service [2].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

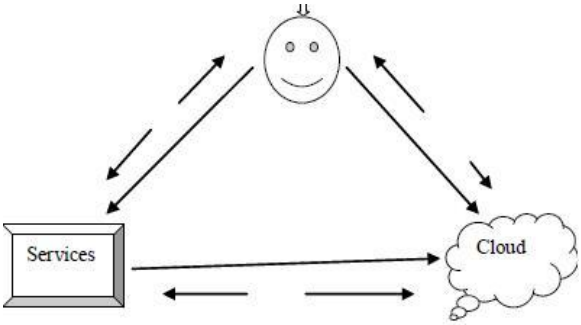

Fig 1: an abstraction of relation between enable, provider and user

This is the depiction of relation between the service provider, the enabler and the user of the services:

Enabler: these are the companies that enable the underlying infrastructures typically focusing on server virtualization like Vmware, Bladelogic, Redhat, Sun, Ibm.

Providers: it includes providers like aws a popular cloud provider by Amazon, Google providing the services by the name of Google App Engine, Rackspace, as well as Microsoft. These companies typically offer the platform or infrastructure.

*Consumers***:** They typically build the applications on using the services or infrastructure. By using various services, paying according to their usage and finding out their business solutions for a wide variety of problems.

.

II. HADOOP INFRASTRUCTURE

There are mainly four types of virtualization (a) Server virtualization (b) Storage virtualization, (c) Network virtualization, (d). Service virtualization. So to protect the information in this virtualization world some techniques are to be implemented. Still there is a scarcity of trust between users using cloud services and the community providing cloud services and this is the reason that is hampering the acceptance of cloud services of outsourced computing services. Now the Hadoop infrastructure was designed to support data profound distributed applications [4]. Due to its design it is highly recommended to support and simulate cloud computing based applications as well as algorithms that are intensive in nature.

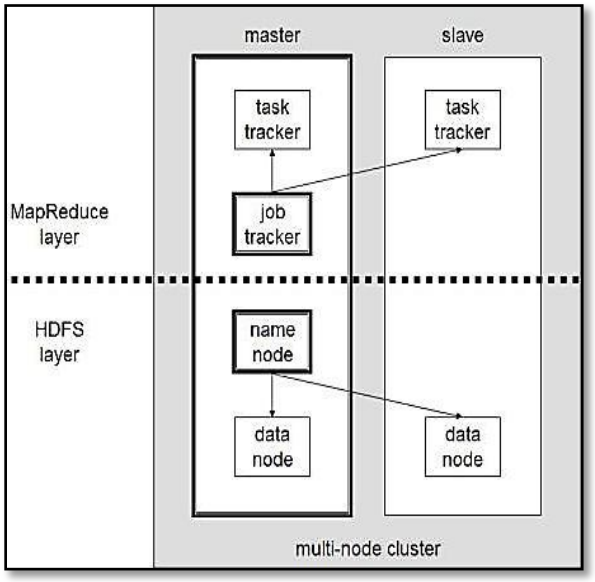

Fig 2: Hadoop Clustering System

With the help of map reduce the Hadoop distributed file system gives support for a software development framework that helps in processing of large datasets. Map reduce in this whole framework supports the watermark computational work. Here the job of data node is to provide data storage services for the shared environment or shared file system. The data node is a node that actually stores the data in a physical file system. Name node: its job is to manage the Meta data about all the clusters as well as data nodes. It also supports the coordination for storing and retrieval of each data block managed by each data node. Generally saying a cluster is comprised of name node and a data node. In the Hadoop architecture, there is one name node and multiple data nodes as depicted in the figure. It can also be said that master is a name node and slaves are data node. Job tracker: it is used when some processing is needed for data. Whenever a job is submitted to job tracker is divides the job and allocate it to various available task trackers when each task tracker process the task. After processing the task it again submit the results to job tracker. Job tracker polls the task tracker weather it is available or not. The advantage of clustering is that whenever one task tracker fails the job tracker reschedules the job and assigns it to another available task tracker.

III. CLOUD IMAGE WATERMARKING

The cloud model: Suppose U is a value expressed in precise quantitative theory of the domain, C is a U on the qualitative concept, if the quantitative value x $\in$U, and x, a random realization, is a qualitative concept C. The certainty of x of C, μ (x) $\in$[0,1] is a stable tendency of the random number. μ: U $\rightarrow$ [0,1], x $\in$ U, x $\rightarrow$ μ (x), then the distribution x in the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

domain U is called clouds, and each x is called a cloud droplet [9]. The digital characteristics of clouds are represented by expect value Ex, entropy En and ultra-entropy He. All of them reflect the concept of Ã as a whole on the qualitative-quantitative characteristics. **Expectation (Ex)**: best representing the concept of Ã the qualitative point in the log-domain space can, or the most typical of the sample points. **Entropy (En)**: on the one hand reflecting the acceptable range of the number of field space which may be accepted, or the ambiguity also reflecting the number of points in domain space representing the probability and its randomness. **Hyper Entropy (He)**: hyper Entropy is measure of the entropy's uncertainty. The size of hyper entropy indirectly reflects the thickness of the cloud. The cloud is made up of many cloud droplets. Due to its uncertainty the cloud also shows the accuracy of the given conceptual point. When the En/He is very small, or super-entropy He is relatively large to the entropy En, the clouds generally take the form of mist. Different En, Ex, He and cloud droplets N can have a different cloud, and different cloud can be used as a watermark embedded in the image.

The cloud formation: The formation of cloud is achieved by software i.e. cloud generator, it is a forward cloud generator and reverse process is the backward cloud generator [8]. Firstly we have to enter all the three parameter Ex, En, He and a cloud droplet number N whereas using the algorithm.

- Produce a normally distributed random value En'_i with mean En and standard deviation He.
- Produce a normally distributed random value X_i and with a mean value of Ex with standard deviation En'.
- Now calculating

$$\mu_{i=-\frac{(x_i-E_x)^2}{2(En_i)^2}}$$

- Drop (xi, μi) is a cloud drop in the universe of discourse.
- Repeat step 1 – 4 until N cloud drops are generated, which form new cloud drops.

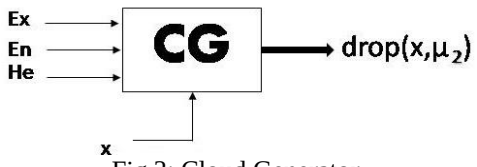

Fig 3: Cloud Generator

Along with the above algorithm, the use of certain programming languages such as C + +, VB, MATLAB, etc. can achieve cloud formation. In MATLAB, the function normrnd is to generate random numbers subject to normal. The code is to generate normal random numbers. Each time providing different sets of values will give different numbers for implementation.

```
x=zeros (1, N);
y=zeros (1, N);
x(1:1000)=normrnd(En,He,1,N);
for i=1:N
En=x(1,i);
x(1,i)=normrnd(Ex,En,1);
y(1,i)=exp(-(x(1,i)-25)^2/(2*En^2));
plot(x,y,'.');
end
```

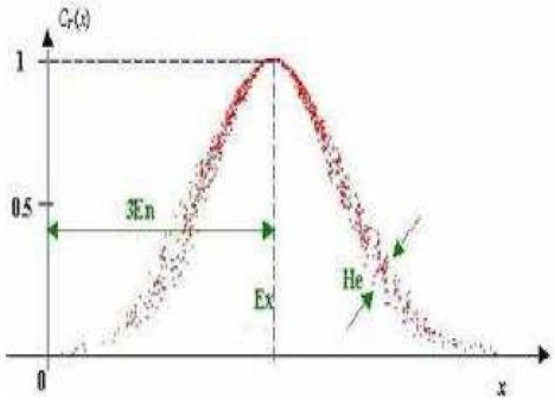

Fig 4: Graph Plotting For Cloud Generator

This figure denotes the digital characteristics of the linguistic terms. Here the thickness of the model is unpredictable or undefined. At the top where the value is 1 and at the bottom where the value is near 0 the degrees are not to dispersed whereas at the waist or slightly above the bottom.

IV. IMAGE WATERMARKING BY DISCRETE COSINE TRANSFORM

After the cloud drops are generated using above method and by calculating the **expectation value**, **entropy** and **hyper entropy**. The discrete cosine transform embeds the watermark in a standard image by adjusting the block DCT coefficient of the image then by blocking the selected image according to 8x8 pixels then dividing the selected image into non overlapped sub image blocks [7].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

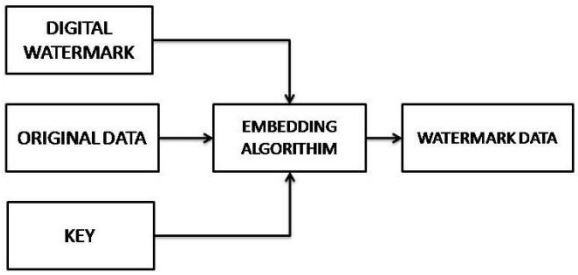

Fig 5: Watermark Insertion

V. WATERMARK EMBEDDING ALGORITHM

- Firstly transform original image X into 256×256 standard image as the original image, pick up the decomposed component get a 128×128 image where the decomposed low frequency coefficient matrix is **A** (128×128).
- For an added watermark equally distributed in 128×128 pixel image, matrix A is blocked by 8×8 size and then make DCT for each block, choose the first value in the matrix composed of DCT transformed coefficient of each block as $\mathbf{F_n(1,1)\ (1 \le n < 1024)}$.
- Read the binary watermark ($1 \le n < 1024$).
- Firstly according to positive direction Z scanning (from left to right and from upper to lower), transform watermark image to the sequence $\mathbf{\{W_k\}}$ as the length of N, create 0～N-1 random sequence $\mathbf{\{r_j\}}$ as random seed of key K and increase it to $\mathbf{\{W_k\}}$ sequence to create a new watermark sequence $\mathbf{W_k}$. The new watermark is embedded in $\mathbf{F_n\ (1,\ 1)}$.

This embedding algorithm ensures that coefficient with larger amplitude in original chart field corresponds to watermark image DCT with larger amplitude. Another issue is that DCT coefficient is comprised watermark image with low frequency information [10].
Hence the image will be secured in the data centers where there is a lack of trust among users and data owners the DCT will work as the key factor in providing robustness against distortion attacks as well as other security threatening attacks

VI. CONCLUSION

Discrete cosine transform algorithm after generating the cloud drops gives the robustness when used in a distributed computing environment. It also ensures that the attacks involved in cloud computing such as distributed denial of services, cloud malware injection attack, side channel attack can be avoided up to some extent. This method also ensures that even if the data is steeled by an intruder or third party then also the copyright protection is achieved as the watermarking is done by shifting the coefficient [3].

VII. FUTURE WORK

This algorithm can be implemented in various cloud datacenter and at which layer the cloud provider wishes is of his own choice but for its efficient use the data must be copyrighted before storing to the datacenter so that when exclusive cloud drops will be generated using cloud generator the user as well as the provider will be satisfied about the performance. The implementation can be done by creating a prototype in apache Hadoop by using a master slave clustering

ACKNOWLEDGMENT

I would like to give a special thanks to my guide Dr. Shaliendra Singh, who always support and encourage me towards this work. He has guided me in all the aspects whether it is technical or non-technical.

REFERENCES

[1] Russell dean vines, "cloud computing software security fundamentals", Indianapolis, Indiana, 2010, ch.3, sec.1, pp.90

[2] Waynejansen, "guidelines on security & privacy in public cloud computing", special publication 800- 144, national institute of standards & technology.

[3] Ajey Singh, Dr. Maneesh Shrivastava, "overview ofattacks on cloud computing, international journal of engineering and innovative technology, vol.1, issue4, april 2012, pp. 321-323.

[4] Chao-Tung Yang, Chu-Hsing Lin**, and Guey-Luen Chang, implementation of image watermarking process on cloud computing environment, spriNGER VERLAG BERLIN PP.131-140.2011

[5] Kai Hwang, trusted cloud computing with secure resources and data coloring, ieee internet computing, 2010 pp14-22

[6] Chu-Hsing Lin, Chen-Yu Lee, Shih-Pei Chien, digital video watermarking on cloud computing, sdiwc, 2013, pp 46-53.

[7] Gengming Zhu, Watermarking Algorithm Research and Implementation Based on DCT Block, World Academy of Science, Engineering and Technology 45 2008, pp38-42.

[8] Yongzhang, xiamuniu, "a method of protecting rdb copyright with cloud watermarking",world academy of science, engineering & technology, pp.68.72.

[9] Zhiguo du, dahuihu, "image watermarking technology based on cloud model", asia pacific youth conference on communication technology, pp.25.27,2010

[10] Yu-chaoliu, yu-tao ma, "a method for trust management in cloud computing: data coloring by cloud watermarking", international journal of automation and computing, pp.280-285, august 2011.