Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.333 – 339

RESEARCH ARTICLE

The Amalgamation of Digital Watermarking & Cloud Watermarking for Security Enhancement in Cloud Computing

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

[1]Department of computer Engineering & application & National institute of technical teacher's training & research Bhopal, India

[2]Department of computer Engineering & application & National institute of technical teacher's training & research Bhopal, India

[1] navneet131088@gmail.com; [2] ssingh@nitttrbpl.ac.in

Abstract— Cloud computing in today's world is making wide differences between it and other technologies. The critical data of users can be stolen by various means whereas cloud computing is still not a secure way to store users data. This paper tries provides a review of what are various types of digital watermarking techniques and in what way the integrity of watermarking can be attacked so as throttle the system. The collaboration of digital watermarking when used for cloud computing can significantly result to make the system robust as well as secure user's data.

Key Terms: - Cloud security; digital watermarking; cloud watermarking; data coloring; bit attack

I. INTRODUCTION

Cloud computing provides the capability to use the storage resources as well as computing resources on usage basis and reduce the investments and expenditures in the organizations computing environment. The creation and deletion of virtual machines running on physical infrastructure and most usually controlled by hypervisors and that is the most important cost effective as well as flexible computing paradigm. It can also be referred to as accessing software, applications and storing the data in cloud representation of internet and also using various services. Some of them also see it as nothing new but just an advanced version of a time sharing model that was widely employed during 60's before the arrival of lower cost computing platforms. Cloud computing has mainly five essential characteristics, three service models and four deployment models. The characteristics are on demand self-service, ubiquitous network access, resource pooling, location independence, rapid elasticity. The services are SaaS- providing applications over a network, Paas- deploying customer created applications to a cloud, Iaas- renting the processing, storage & network capacity. The deployment models are Private cloud- enterprise owned, community cloud- shared infrastructure to a specific community, public cloud- sold to public, hybrid cloud- composition of two or more cloud. The cloud computing also provides some exclusive features that are far more useful than a centralized sever model. They are: (1) *Scalability on demand*- An organization has to deal with a dynamic situation where sometimes the computing resource needs to be much higher and in some scenario doesn't need much resources, the cloud computing has that ability to scale the resources up as well as down. (2) *Streamlining the data center*-Organizations can make their data centers to simplify the working process i.e. transferring the workload over the cloud data centers. (3) *Meliorating business processes*- The suppliers and partners can share the applications and data in a cloud environment, this helps in focusing on business processes rather than implementation that is hosting it [14]. (4) *Minimization of startup cost*- Cloud

computing heavily reduces startup cost; it is helpful for the organization that is emerging in markets and also for and advanced technology groups that are the giant and most importantly for the starters that are just starting out their organization [1].

Remaining section of the paper is organized as- section 2 introduces to various cloud computing security issues & objectives. Section 3 is the discussion about digital watermarking and its various uses in real world computing. Section 4 is about critical security threatening issues related to digital watermarking. Section 5 & 6 combines the digital watermarking technology with cloud computing. Finally the paper is summarized by an overview of survey and further scope.

II. CLOUD COMPUTING SECURITY

The concern is for security in cloud computing environment when passing on any organizations critical information to geographically dispersed cloud platforms and that too is not in control of that particular organization whose data is to be stored on a cloud platform [2].Security issues related to the security of cloud computing are-

1) *Privileged access*: This is the question about who has the privilege to access the data. Who is Responsible for hiring & management of the administrators, which handles the information?

2) *Separation of the data from its actual location:* How the encryption is performed, who is responsible for encryption & at which layer the encryption is done.

3) *Data availability:* Can the cloud vendor move entire data to a different location or environment and should the existing environment must be compromised [10].

4) *Regulatory compliance:* It is the choice of the cloud vendor, whether willing to undergo external audits or security certificates.

5) *Long term viability:* This is the critical issue, what happens to the user's useful data when the cloud vendor goes out of business, does the data is returned back to client and if returned what is the format of the data.

Security concerns based on delivery and deployment models are data integrity, data locality, data confidentiality, and data access. Some more security related concerns are Sign on process, Authentication & authorization, network security, identity management [3]. Objectives of cloud information security According to "data and analysis center for software" (DACS), a software must exhibit these three properties. Trustworthiness- Any software that is resistant to malicious logic is mainly the objective of achieving trustworthiness. Software should have minimum number of vulnerabilities that is mainly responsible for slowly damaging software's dependability. Dependability- Software must operate correctly under various conditions that also includes running on malicious host. Resilience- Software must be resistant to the attacks and also must have an ability to recover from the damage as quickly as possible [4].Some of the security management environment and possible threats are:

A. Virtualization security management

The virtual machine, virtual memory manager, hypervisor or hosts are least number of components required to setup a virtual environment. Virtual threats are threats to a virtualized environment are generic in nature such as denial of service attack. There are some other threats that are unique to virtual machines [12, 15]. The fact is that vulnerability in one VM system can be exploited to harm or intrude other VM, this is because multiple virtual machines share same physical infrastructure.

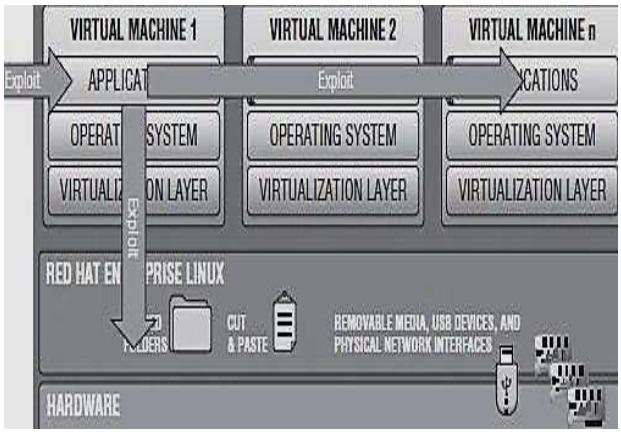

Fig. 1: VM system vulnerability

B. Trusted cloud computing

It is can be viewed as security architecture designed to protect cloud systems from various malicious intrusions and attacks to ensure that the computing resources will execute in a predictable manner as it was designed.

C. Trusted computing base (TCB)

It is the total combination of protection which includes hardware, software and firmware, trusted to enforce a security policy. TCB must also provide for memory protection to ensure that the process from one domain do not access memory location of another domain.

D. Trusted platform module (TPM)

It is used to store cryptographic keys that are used to attest to operating state of computing platform to ensure that the hardware and software configuration has not been modified [11].

III. WATERMARKING AND APPLICATIONS

A watermark is mainly a type of information that is embedded with the data so as to avoid its manipulation, to verify for ownership proof. Widely used watermarking is on still images, videos, and mostly on audios. Depending on the type of data to be watermarked various algorithms are used such as patchwork algorithm used for image watermarking, there are various other algorithms used for various purposes like airspace algorithm, Nippon algorithm. Watermarking generally consists of two phases; watermark embedding i.e. introduce small images or pattern into the data without affecting the original data. A key is used to embed the watermark information into the data; once the watermark information is embedded the data is available for the use. Another phase is watermark detection or verification this phase is used to verify the ownership of the data. The data is compared with the suspicious database using the same key.

Image watermarking is mostly used scheme for data that contain image files, the image watermarking uses a private key and one algorithm, for image watermarking we use patchwork algorithm embedding the logo in the original data to form a new image that will be more secure than original data. In normal circumstances if the attacker attempts to alter the watermarking information "I", still the image that is watermarked will be available to intended user. Watermarking detection is performed in two ways, one is we to perform full search and apply hypothesis test to the embedded information, and another one is that the original information can be extracted and verified.

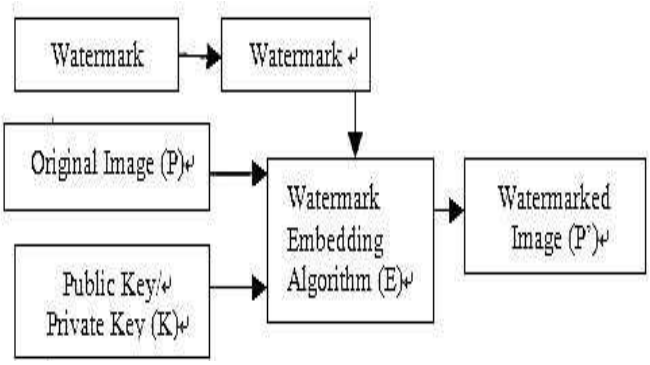

Fig. 2: embedding image watermark

The applications of digital watermarking are as follows-

A. Tamper detection

When the watermark is embedded in the data and stored in the database. Now when the database is retrieved a unique key is used with the source data and in this way the integrity of data is achieved by verifying against the integrity of extracted watermark.

B. Fingerprinting

It helps to identify an intruder; whenever the data is available publically the owner of the data would like to restrict the data to any unauthorized user over the network. Each time a data is travelled over the network a distinct logo is embedded in order to prevent its illegal use. If at any point of time an illegal copy of data is found, the original copy can be determined by fingerprinting [8].

C. Ownership assertion

User A can make the data publically available by adding the watermark information using a private key. Whenever user B attempts to use that data it must have the legal access rights to use the data. Now if user B somehow attempts to claim over that data then to defeat user B's ownership, user A can compare the attributes of both his data as well as user B data. This way user B can be caught about claiming an illegal data.

D. Document security

Digital watermarking technology enables to embed a digital identification into critical documents and images as soon as it is created. The data that is contained in a watermark can be the information related to original source or owner of the data, the information related to recipient and most important if the data is leaked out it can be easily traced back to original sender reporting about the unauthorized use of the document.

E. Regaining online content with digital watermarking

The watermarks can be embedded into all types of contents i.e. image, audio, video. Watermark is the secret information that cannot be seen or heard by humans but computers can easily detect them. There are various internet search services that help in locating uniquely watermarked content. Reports are then generated and informed to the owner of that data about its usages [5].

IV. SECURITY THREATENING ATTACKS

Broadly classifying robust watermarking is used for copyright protection and fragile watermarking is used for integrity verification. Fragile watermarking scheme must be frail enough to detect modifications so as to locate the actual place of data modification under different attacks. Whereas the robust watermarking attacks attempts to distort the watermarking information using various techniques [13]. The watermarked data may suffer from intentional as well as unintentional attacks that can remove damage or even erase the watermark. Some of them are-

A. Bit attack

This attack attempts to distort the watermark information by manipulating the bits i.e. by changing one or more bits, the more an attacker knows about the position of the marked bits more the chances of attacking. If more bits are altered then it can also make the data completely useless. Another variant of bit attack are bit

flipping attack and randomization attack. Bit flipping attack is performed by just flipping the bit or inverting the values of bits position, whereas when attacker assigns random values to certain bit position then the randomization attack is performed [6].

B. Subset attack

Considering a subset of tuples of a watermark relation in a database and attacking on them may give a chance of losing the watermark.

C. Subsets reverse order attack

Attacker can perform this attack by interchanging the order of tuples in any relational database that can distort or even can erase the database.

D. Brute force attack

By Guessing the private key an attacker can traverse the possible search spaces of various parameters.

E. Superset attacks

Some new tuples are added to the database where the watermarking information is stored that can affect the actual detection of watermark.

F. Protocol attacks

This attack aims at creating the ambiguity among the true ownership of the data and some other user other than the true owner claims over the data. This type of attack is called as invertible watermark where the attacker subtracts his watermark from the watermarked data and claiming to be the owner of the data.

G. Cryptographic attacks

Gaining the information about what type of security scheme is used during watermarking. By collecting the security information an attacker can remove the watermark information or can attempt to change the state of watermarking information. This turns to mislead the original owner of the data by modifying the information about original file.

V. THE CLOUD MODEL

This model is a transform of quantitative and qualitative data. Suppose U is a universal set of numbers, C is a qualitative concept related to the universal set U. Any variable x that belongs to universal set U i.e. $x \epsilon U$ randomly realized the concept C with the certainty degree of x for C.

A random value lies between 0 and 1 [9].

$$\mu: U \rightarrow [0,1], \quad \text{for all } x \epsilon U \quad x \rightarrow \mu(x)$$

The distribution of x on U is defined as a cloud and every x is defined as a cloud drop. In this model, the property of cloud drops is represented by Ex i.e. expected value, En i.e. entropy and He i.e. hyper entropy where expected value is a mathematical representation of cloud drop. We can also say that a cloud drop is located at some point Ex is most recognizable value of qualitative concept. En connects the concepts of both randomness and fuzziness by granularly measuring the qualitative concept. He is the uncertainty measurement of entropy i.e. entropy of entropy, showing to what degree a cloud drops form a common concept. This limits that if He<En no longer a concept can be formed.

VI. DATA COLOURING TECHNIQUE

The difference between traditional watermarking and cloud watermarking is that in cloud watermarking it just not only embeds the user's copyright information but it also colors all of its data. Each of the users is specified with a color that helps to protect the copyright and also avoids the manipulation of original data. The procedure of data coloring is followed by specifying the 3 parameters that were discussed in previous section i.e. En, He, Ex and Ex is always provided by the owner of that specific data [7]. En and He are the result of negotiation of the service provider and data owner

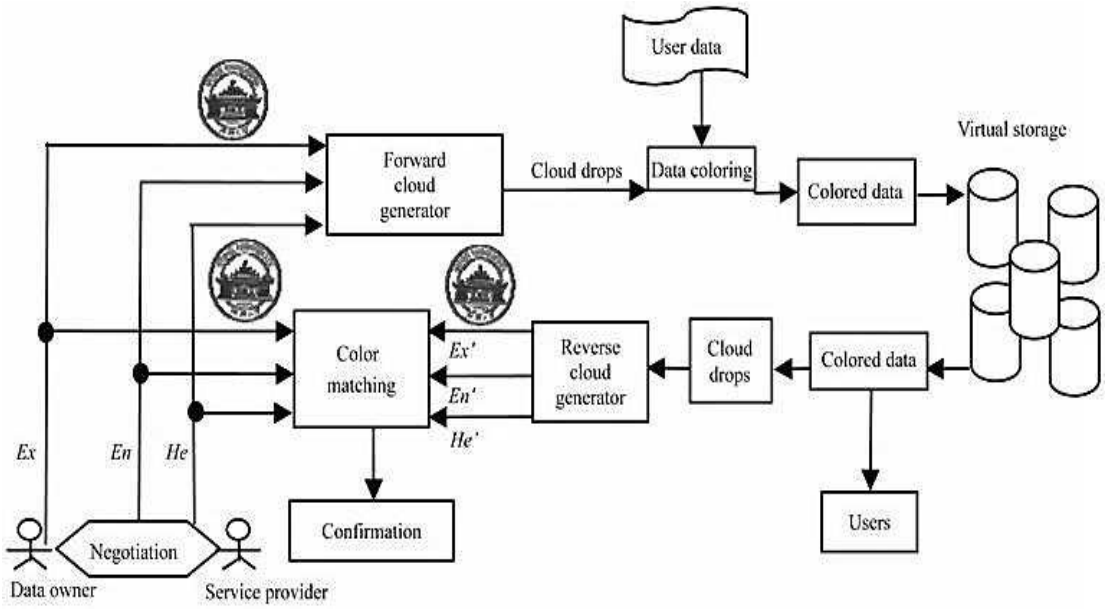

Fig. 3: data coloring with cloud watermarking

Now after value negotiation the cloud drops are generated using the forward cloud generator algorithm. The compliment of the forward cloud generator is the reverse cloud generator algorithm which is used to extract the cloud drops from colored data. At last the color matching will confirm the original owner of the data. This data coloring method is helpful in securing documents, images as well as relational databases. The color matching process here aims to correlate the colored data object with its owner. The data coloring technique can be applied at various levels depending on the cost. On combining the technology of data coloring with secure data storage we can prevent the objects from being altered, modified, erased, hacked and stolen. Any cloud platform that is at risk can cause a more losing business as well as disrupting or even causing a huge loss to public services. Intruders can enter a secure system by means of various malware attacks like viruses and worms. This data coloring method can be implemented at data center access at course grain level as well as secure data access at fine grain level. This will make the architecture more usable if the user data will be access at fine level that is complex at developer's site but not at user's site. Still this implementation has a drawback that is there will always be a time complexity issue between the data extraction at user's site. Each time the user has to wait for the negotiation, so that the color granularity must be first exact as the previous one when the data was uploaded to data center.

VII. CONCLUSIONS

We have covered the threats related to cloud computing security and the overall effect on whole system when a single virtual machine is been attacked. The digital watermarking techniques that is helpful for cloud security. This topic opens number of opportunities for future exploration. The various threats that can harm the integrity of watermark information have been highlighted. The way the cloud computing security can be enhanced using the cloud watermarking concept is having a huge scope to deal with. In future we would like to implement this technology to measure its parameter and analyze its contribution in securing the cloud computing environment, whereas improving the time complexity while the negotiation takes place, by improving the working structure of backward cloud generator we can improve this model.

ACKNOWLEDGEMENT

This paper is combined effort of me and my guide dr. shailendra singh, who has always been cooperative in supporting for making this paper. He has also actively guiding in improving all the aspects weather it is technical or non-technical issues of this paper. I would like give special thanks to my guide, without his efforts it won't be possible for me to complete this paper.

REFERENCES

[1] Ronald L. krutz, "cloud computing fundamentals", what is cloud computing, Indianapolis, Indiana, 2010, ch.1, sec.1, pp.26, 30-32.

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

[3] Amandeep Verma, Sakshi Kaul, "cloud computing security issues & challenges: A survey", springer-verlag berlin Heidelberg, part IV, ccis 193, pp.445-454, 2011.

[4] Ronald L. krutz, "cloud computing software security fundamentals", cloud information security objectives, Indianspolis, Indiana, 2010, ch.3, sec.1, pp.91-92.

[5] zhiguo du, dahui hu, "image watermarking technology based on cloud model", asia pacific youth conference on communication technology, pp.25.27,2010.

[6] agostino cortesi, shantanu pal, "watermarking techniques for rbd: survey classification & comparison", journal of universal computer science, vol.16, no.21, pp.3164-3171, 2010.

[7] yu-chao liu, 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.

[8] Michael Arnold, martin schmucker, "applications of digital watermarking", copyright protection, library of congress cataloging, isbn 1-58053, ch.3, pp.40.

[9] yong zhang, xiamu niu, "a method of protecting rdb copyright with cloud watermarking", world academy of science, engineering & technology, pp.68.72.

[10] akhil behl, "emerging security challenges in cloud computing", world congress on information and communication technology, pp.217-218, 2011.

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

[12] joshi akshay "enhancing security in cloud computing", information & knowledge management, vol.1, no.1, pp.40-43, 2011.

[13] Cyril bazin, jean marie, "a novel framework for watermarking", springer-verlag berlin Heidelberg, pp.201 217, 2008.

[14] priyanka arora, himanshu tyagi, "evaluation and comparison of security issues on cloud computing environment", world of computer science and information technology journal, vol.2, no.5, pp.179-183, 2012.

