# A SURVEY ON WATERMARKING METHODS FOR SECURITY OF CLOUD DATA

**Mrs. Anitha P[1], Dr. Malini M Patil[2]**

[1.2]*Department of Information Science and Engineering, JSSATE (India)*

## ABSTRACT

*The paper emphasis on the concepts of cloud computing and its related methodologies with respect to the security aspects of cloud data. Main aim of this paper is to present the survey of cloud computing techniques, to study about Security issues and the need and importance of digital watermarking in securing cloud data. The work gives an overview of the literature survey for secure cloud computing and discusses about issues and challenges involved for storing the cloud data . An overview of encryption methods and watermarking approach for secure data storage are also presented.*

***Keywords: Adoptability, Agility, Encryption, Scalability, Watermarking.***

## I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous network access, on demand self service, pay-for-use, and economies-of-scale IT services over the internet. In [2], the author explained that computing will become a utility like a telephone . But the idea of the author was found to be impractical due to lack of infrastructure. In [13] the author defines cloud computing as the approach of computing which deliveres IT facilities 'as a service' to end users through internet. Sales force during 1999 launched first cloud computing product. Amazon, Google, Microsoft and few others have offered cloud based products and services to the market. In[4] author defines cloud computing as an internet based computing which refers to both the applications delivered as services as well as network and system softwares.

The rapid advancement of cloud computing has gain the popularity across world wide web. Normally the cloud looks like a big black box, content is invisible to the clients so the clients have no idea or control over what happens inside a cloud. It may result in the violation of confidentiality and integrity of the system. Many organizations are shifting towards the cloud computing systems for the storage of resources rather than using local storage. This resulted in virtualization as demand for shifting various applications to cloud increased. Simaultaneously this activity resulted in handling security issues in cloud computing. Fig [1] shows the structure of cloud computing used in IT organizations and is self explanatory.

To overcome the security issues, scientists launched a variety of methods and policies for protecting content copyright and strenthening security for safe transmission of data by avoiding attacks from malicious third parties. Among different techniques suggested , digital watermarking is considered to be very useful for data protection and authentication. Digital watermarking is a technique to protect host digital data by embedding the data property like the company logo/image, copyright information into data . Then the object is called as a watermarked object. The hidden data may be visible or invisible to verify the ownership of intellectual products.

The paper is organised as follows. The overview of cloud computing is discussed in section II of this paper. Section III is about cloud computing characteristics . Section IV is about different methods of security aspects in Cloud.,Especially it deals with encryption and watermarking methods for data security in cloud. Section V gives some challenges in cloud environment and finally conclusions are discussed in Section VI.

## II. CLOUD COMPUTING OVERVIEW

The cloud computing name was inspired by the symbol of cloud that is often used to represent the internet in diagrams and flowcharts[3]. Cloud computing is a model for accessing shared pool of configurable computing resources (e.g., networks, storage,servers, services and applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Fig 1 explains how IT organizations are impacting on cloud computing**.**By making data available in the cloud, it can be more easily accessed world wide often at much lower cost, increasing its value by enabling opportunities for enhanced collaboration, integration, and analysis on a shared common platform.

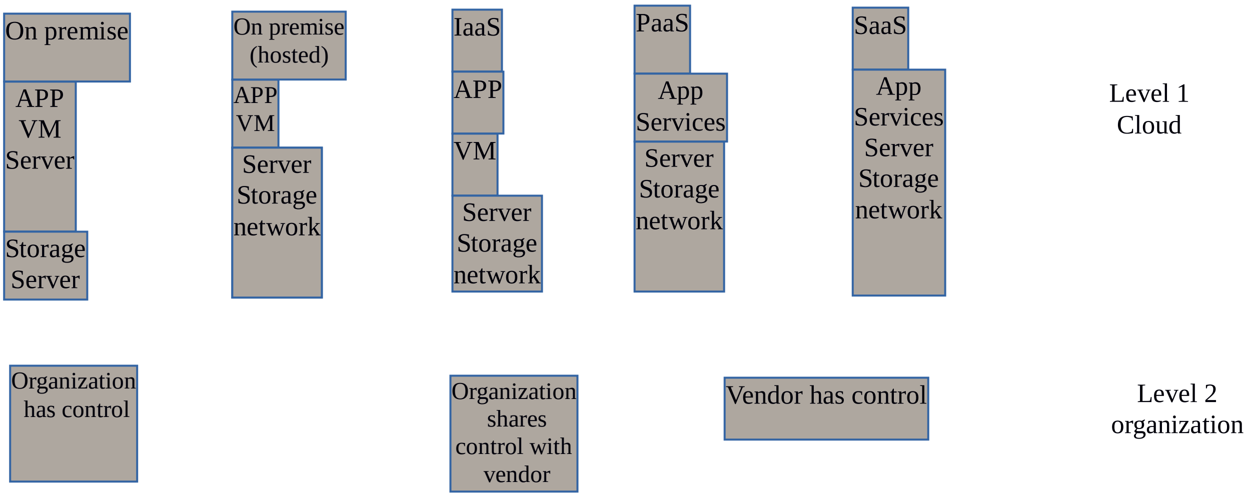

**Fig.1 Impact of cloud computing on the structure of Information technologies.**

### 2.1 Service Models of Cloud Computing

The three service models/delivery models available in cloud computing are

1. SaaS (software-as-a-service): Consumer has a capability to use the provider's applications running on a cloud infrastructure. Using thin client interface, applications are accessible from client devices like web based email. Examples for SaaS are Google Apps, Salesforce.com, WebEx etc.
2. PaaS (platform-as-a-service): PaaS Provides the consumer with the capability to deploy onto the cloud infrastructure(middleware,databases) ,Consumer created or acquired applications, produced using programming languages and tools supported by the provider .The consumer has a control over the deploy applications but not on the cloud infrastructure[5].Examples for PaaS are Coghead, Google Application Engine, AWS Elastic Beanstalk, Windows Azure etc.
3. IaaS (infrastructure-as-a-service): IaaS provision the consumer with the Computational capabilities to processing, storage, networks, and other computing resources in a centralized, location transparent services and allow the consumer to deploy and run arbitrary software, which can include operating systems and

applications. Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Joyent etc.

### 2.2 Cloud Deployment Models

Cloud computing architecture identifies 4 deployment models as described below:

1. Private cloud: The cloud infrastructure is operated for a private organization. It is managed by the organization or a third party, and may exist on premise or off premise.
2. Community cloud. The cloud infrastructure is shared for specific community or shared by several organizations that has communal concerns (e.g., mission, security requirements,policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist single tenant.
3. Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services(multi-tenant).
4. Hybrid cloud. The cloud infrastructure is a combination of two or more clouds (private, community, or public) that are bound together by standardized or proprietary technology, but remain as a unique entities that enables application and data portability (e.g., cloud bursting for load-balancing between clouds) [6]

**Table 1: Cloud service models with security requirement and threats.**

| Type of service | Users | Security requirements | Threats |
|---|---|---|---|
| SaaS | End Users | 1. Access control<br>2. Privacy in multitenant environment<br>3. Communication protection<br>4. Software security<br>5. Service availability | 1. Impersonation<br>2. Modification of data at rest and in transit<br>3. Session hijacking<br>4. Traffic flowc analysis<br>5. Interception |
| PaaS | Developers &moderators | 1. Access control<br>2. Security for application<br>3. Security images<br>4. Virtual cloud protection | 1. Programming flaws<br>2. Software modification<br>3. Session hijacking<br>4. Traffic flowc analysis |
| IaaS | System owners | 1. Hardware reliability<br>2. Hardware security.various<br>3. Network protection<br>4. Abuse use of cloud | 1. DDOS<br>2. Connection flooding<br>3. Interruption<br>4. Network attacks |

## III. CLOUD COMPUTING CHARACTERISTICS

The 5 main essential characteristics of cloud computing are as shown in the Fig 2 are discussed as follows according to [20].

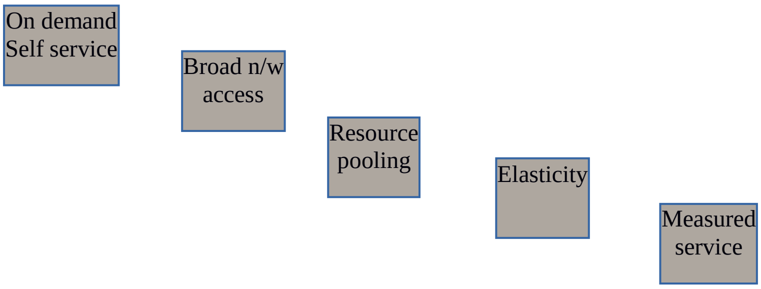

**Fig 2:cloud computing characteristics**

1. On demand Self Service: Organization has access to services and power to change cloud services through an online control panel or directly with the provider. They can add or delete users and change storage networks and software as needed. Typically, they are billed with a monthly subscription or a pay-for-what-you-use scenario. Terms of subscriptions and payments will vary with each software provider.

2. Broad network access: It includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment. This mobility is particularly attractive for businesses so that during business hours or on off-times, employees can access/stay on top of projects, contracts, and customers wherever they are. Organization can access the resources using tablets, laptops, mobiles, office computers etc.

3. Resource pooling: The cloud enables organizational employees to enter and use data within the business management software hosted in the cloud at the same time from any location and at any time. This is an attractive feature for multiple business offices and field services that are outside the office.

4. Elasticity: Resources can be used by clients based on their requirements from the cloud by scaling out and can scale back in by discharging the resources if they are no more needed.

5. Measured Service: The amount of resources that are used can be monitored and controlled in terms of CPU hours, bandwidth usage, storage usage etc.

## IV. SECURITY IN CLOUD COMPUTING

Privacy is the main consideration due to shared environment of cloud computing, processing of data, remote access, combined service and information flow across provider boundaries [7]. The mechanisms that are used to preserve privacy are Identity and access management.

1. Access management: Access to various services and resources are controlled through mechanisms such as authentication and authorization mechanisms.
2. Identity: In authentication, identity of an applicant is verified and authorization access level is controlled.

Cloud environment consists of multiple services and domains and each domain contains its own access policy. It is needed to design an access control framework that integrates access policies of multiple domains. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML) and web service standards are various frameworks for cross-domain access specification and verification [8]. Organizations and public cloud providers trust each other through identity federation and by sharing digital identity along with the attributes in the same manner supports single sign-on [9]. Identity federation Can be accomplished using SAML and OpenID standards [9]. XACML uses a XML-base language which defines policies and decision making task.

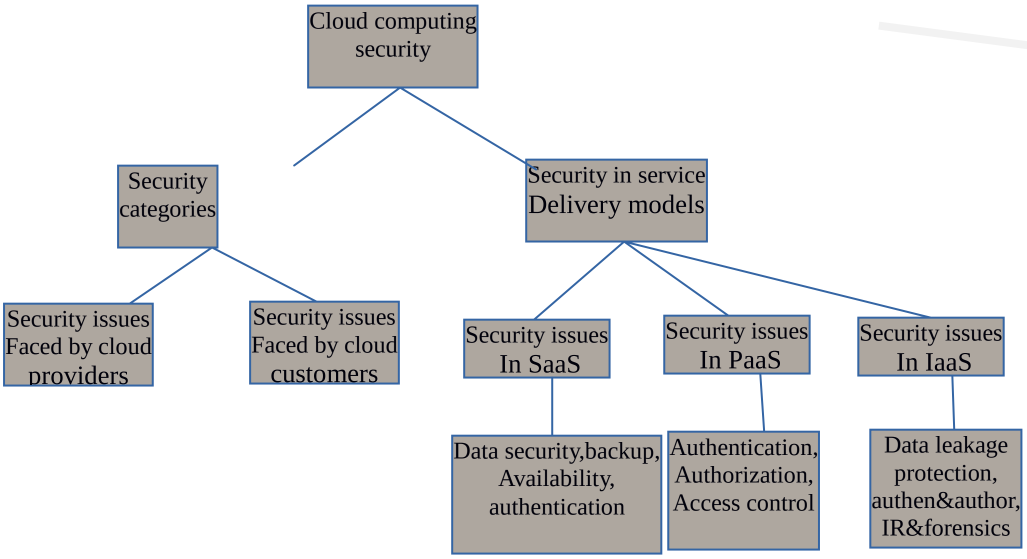
Cloud computing security
Security categories
Security in service Delivery models
Security issues Faced by cloud providers
Security issues Faced by cloud customers
Security issues In SaaS
Security issues In PaaS
Security issues In IaaS
Data security,backup, Availability, authentication
Authentication, Authorization, Access control
Data leakage protection, authen&author, IR&forensics

**Fig 3: cloud computing security layers**

Data integrity, User confidentiality, and Trust are the three Critical security issues among providers, individual users, and user groups. The three most popular cloud service models which are varying in security demands are IaaS, PaaS and SaaS. Traditional integrity checking techniques such as hashing cannot be applied to computation and data integrity in cloud computing, because hashing of such large volume of data through internet is not feasible. Provable Data Possession (PDP) approach can support integrity check in cloud computing. For preserving confidentiality traditional techniques cannot be applied because of threats existing inside the system. Mainly there are 2 types of threats : Fraudulent Resource Consumption (FRC) attack and Flooding attack via bandwidth starvation[10]. Trust is a social problem which is not purely a technical issue. However, user believe that technology can enhance trust, justice, reputation, assurance and credibility in Internet applications.

Cloud providers and researchers need to provide the suitable algorithms and techniques to address the following questions:

- How service providers secure the exchange of messages as well as SLA’s, data and applications during migration to cloud and interclouds?
- How cloud providers can envision attacks to the system before an incident happens and how users can contribute to cloud services in order to rapid detection and protection of data leakages ?
- How to develop an secure system to monitor and measure security performance of cloud offered services from different vendors to choose the most appropriate secure solution based on the target goals of clients?
- What are the techniques that can be used in order to preserve privacy in multi tenant cloud computing environments?
- Some of the cloud-specific algorithms to verify user identities for protect a system from security threats.

### 4.1 Encryption Methods For Data Security in Cloud Computing

The widely used method for data security in cloud computing is encryption techniques[11].The security solutions rely on encryption methods for protecting user's data stored using a services offered by cloud providers[12]. Modern encryption techniques which uses the random number generator method are RC4(rivest cipher), RC6, MARS, AES(advanced encryption standard), DES(data encryption standards), 3DES, Two-Fish, and Blow-Fish. The performance evaluation for the mentioned techniques has been carried out by measuring the speed in both cloud computing and traditional desktop environments[14]. It is very much important for the cloud users to ensure that their data which are being stored in a cloud environment must be safe and secure[15]. So the security is applicable foe both data stored and the data transferring. In order to handle this kind of problem data at both user and server end must be in an encrypted form.

**IaaS encryption[19]**:

- Instance managed encryption: The encryption engine runs within the instance, and the key is stored in the volume but protected by a keypair.
- Externally managed encryption: The encryption engine runs in the instance, but the keys are managed externally and issued to the instance on request.
- Proxy encryption: In this model volume is connected to a special instance or appliance/software, and then connect instance to the encryption instance. The proxy handles all crypto operations and may keep keys either external or onboard.

**PaaS encryption[19]:**

- Client/application encryption: Data is encrypted in the PaaS /client accessing the platform.
- Database encryption: data is encrypted in database and supported by database application
- Proxy encryption: Before sent to the platform data is being sent through an encryption proxy.
- other: Since PaaS is very diverse, additional options includes API's built into the platform, encryption services and other variations.

**SaaS encryption[19]:**

- provider managed encryption: Data is encrypted in the SaaS application and managed by the cloud provider.
- proxy encryption: Data passes through a proxy encryption before being sent to the SaaS application.

## 4.2 Overview Of Digital Watermarking

Digital watermarking is a communication method in which the information is embedded directly and ephermally into digital data e.g., image, video, or audio signals, also called original data or host data to form watermarked data. Watermarking can be defined as a group of bits inserted into a digital data( audio or video or image) file that identifies the file's copyright information (author, rights ). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery.

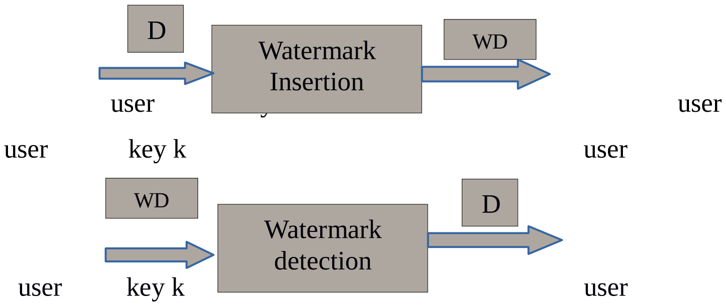

**Fig 4. Watermarking technique**

The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format. So according to the Fig 4 there are 2 phases in watermarking technique:In phase 1 user adds his dataset (D) along with a private key(K). watermark is calculated and available as watermark data(WD). In phase 2. the embedded watermark is extracted by giving Watermark dataset and his private key. So the original data (D) will be extracted with proof of ownership.

### 4.3 Digital Watermarking Techniques

Digital watermarking techniques are classified according to documents types such as:

1. Text Watermarking: It is an approach for text document copyright protection. Digital watermarking for text documents are primarily classified into 3 types.

- Line shift coding : which vertically shifts location of text lines to encode the document.
- Word shift coding: which horizontally shifts location of words to encode the document.
- Feature coding: which will choose certain features and alerts those selected features.

2. Image Watermarking:In this method a watermark is added to image derivatives. The watermark is a part of the image and cannot be easily removed from a picture.
3. Video Watermarking: This involves embedding cryptographic information derived from frames of digital video into the video itself. Ideally, a user watching the video cannot perceive a difference between the original, unmarked video and the marked video, but a watermark extraction application can read the watermark and obtain the embedded information. Because the watermark is part of the video, rather than part of the file format , this technology works independently of the video file format .
4. Audio Watermarking: In this method an electronic identifier is embedded in an audio signal. Some authors proposed the use of text or images to be embedded in the audio file such that any of such audio file could be analyzed for a possible recovery. Some of the audio watermarking techniques available are spread spectrum,amplitude modification,replica method,dither watermarking and self marking methods.

Low[14] proposed 3 kinds of methods which includes line shift coding,word shift coding and feature encoding. The text watermarking algorithms are mainly based on these methods. Semi-fragile watermarking scheme proposed by zhou[15] for content authentication of text documents. The study of watermark figures out that most of the embedded information is image /logo,except from easy watermark creator[16], siotra watermark[17] and watermarkIt[18] which are hiding text as watermark besides images. Most of the watermarking softwares are either shareware or commercial. The cost of an application depends on type of host image, working environment ,type of information embedded etc. Compare to image watermarking ,audio watermark tools are very few. Most of them are freeware. Most of the audio applications are much expensive compare to image applications. The formats of host audio supported are like WAV,MP3,PCM,WMA,WMV etc. video watermarking applications are very rare in the internet. There are many programs found in video watermarking ,all of them are larger compared to both text,image and audio applications.

## V. SECURITY CHALLENGES OF CLOUD COMPUTING

The author in [21] defines privacy as “privacy entails the applications of policies,laws,processes and standards by which personally identifiable information(PII) of individuals is managed”. Authors believe that security is the main key challenge of cloud computing and there is a lack of new cloud specific methodologies and techniques in connection to security. Following are some of the challenges need to be addressed in cloud computing are

1. How cloud providers exchange the messages securely as well as SLA's and transits of data and applications during migration to clud and inter clouds.
2. Cloud providers need to predict attacks to the system prior and how users can contribute to cloud services for rapid detection and protection of data leakages.
3. To verify user identities, new and cloud specific algorithms need to be designed for protecting a system from security threats.

## VI. CONCLUSION

One of the major challenges in the cloud computing is security. The paper discusses on the survey of cloud computing characteristics, emerging security issues for service models and security aspects for deployment models. Second phase of the survey is carried out on the need and importance of digital water marking techniques in cloud security. various digital watermarking techniques are studied with respect to authentication for cloud data. Future work is about the critical study of a digital watermarking as a security aspects for different techniques, algorithms visualization of teh same to the cloud computing system.

## VII. ACKNOWLEDGEMENT

The authors of the paper acknowledges JSSMVP's JSS Academy of technical education, Bangalore for providing facilities to carry out the research work.

## REFERENCES

[1]. Amandeep verma ,sakshi kaul ,”Cloud computing Issues & challenges :A survey “, Springer verlag Berlin Heidelberg, part IV,ccis 193,2011,pp.445-454.

[2]. Abelson, Hal, ed. Architects of the InformationSociety, Thirty-Five Years of the Laboratory for ComputerScience at MIT. MIT Press, 1999, ISBN 978-0262071963.

[3]. Dimitrios Zissis ∗ , Dimitrios Lekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece.

[4]. Michael Armbrust, “A View of cloud computing”

[5]. Addressing cloud computing security issues Dimitrios Zissis ∗ , Dimitrios Lekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece journal homepage: www.elsevier.com/locate/fgcs.

[6]. National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009, csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[7]. C.N. Höfer and G. Karagiannis, “Cloud computing services: taxonomy and comparison,” Journal of Internet Services and Applications, 2011, pp. 1–14.

[8]. D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, “Not so different after all: A cross-discipline view of trust,” Academy of Management Review, vol. 23, no. 3, pp. 393– 404, 1998.

[9]. S. Bradshaw, C. Millard, and I. Walden, “Contracts for clouds: comparison and analysis of the Terms andConditions of cloud computing services,” International Journal of Law and Information Technology, vol. 19, no. 3, 2011, pp. 187–223.

[10]. Research Challenges and Prospective Business Impacts of Cloud Computing: A Survey, The 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 12-14 September 2013, Berlin, Germany

[11]. Encryption Techniques for Cloud Data Confidentiality, international Journal of Grid Distribution Computing Vol.7, No.4 (2014), pp.11-20 http://dx.doi.org/10.14257/ijgdc.2014.7.4.02

[12]. Adeela waqar,asad raza,haiber abbas,Muhammad khurram khan,”A framework for preservation of cloud users dataprivacy using dynamic reconstruction of metadata”. Journal of network and computer applications .www.elsevier.com/locate/jnca.

[13]. Gartner, “What you need to know about cloud computing security and compliance”, (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013).

[14]. S.H.Low ,N.F.Maxemchuk,”capacity of text marking channel,”IEEE signal processing letters ,2000,pp.345-347

[15]. Z.Jalil,A.M.Mirza,T.Iqbal,”A Zero watermarking algo for text documents based on structural components,” Inproceedings of international conference on information and emerging technologies,2010,pp,14-16.

[16]. http://www.easyimagetools.com

[17]. http://www.softsea.com

[18]. http://www.watermarksoft.com..

[19]. Cloud security alliance, “security guidance for critical areas of focus,”dec 2009.[online].available:http://www.cloudsecurityalliance.org/csaguide.pdf

[20]. “An efficient approach for software protection in cloud computing”,2014 4th international conference on communications and network technologies.

[21]. S.Pearson, “Taking account of privacy when designing cloud computing services,” in software engineering challenges of cloud computing,2009.CLOUD'09.ICSE workshop on 2009,pp.44-52.