IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ensuring Security And Ownership Detection In Cloud Computing

B.L. Devi[1], S.K. Das[2], N. Dash[3]

[1]Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.

[2] Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.

[3] Assistant Professor, Dept of CSE, GITAM, Bhubaneswar - 752054.

ABSTRACT:- In cloud computing, resources are centralized and provided to customers via the internet using virtualization technology. This allows for dynamic, scalable, and virtualized resources. Cloud computing offers supercomputing and massive storage, but security remains a key concern, particularly in managing trust between data owners and storage providers. Cloud security focuses on ensuring trust between data owners and storage providers. It's important because data owners worry about how their data will be used or shared without their permission. Choosing data storage services in the cloud becomes a social challenge reflecting human interactions online. To manage trust between data owners and storage providers, we propose using a technique called cloud watermarking with the color drop method. This technique aims to identify and ensure ownership of data stored in the cloud.

Keywords ---- Cloud Computing, Cloud Security, CORDS , Ownership Protection, Cloud Watermarking, Colour Drop.

1. INTRODUCTION

Cloud computing is Internet-based computing in which pooled resources, software, and information are made available to users as needed, much like how the electrical grid works. The provisioning of dynamically scalable and frequently virtualized resources as-a-service over the Internet is typically involved in it. It describes a new consumption and delivery model for IT services based on the Internet. Customers rent resources from a third-party supplier instead of purchasing or maintaining the physical infrastructure, which saves them money on capital expenses. They use resources as a service and only pay for what they really use.

The National Institute of Standards and Technology (NIST) defines cloud computing as a delivery model for IT services as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with little management effort or service provider interaction."

NIST specify five characteristics of cloud computing

On-demand self-service includes users ordering computing resources, like more computers, network bandwidth, or user email accounts, through a website or a similar control panel interface without interacting with the vendor directly.

Broad network access enables users to access computing resources from a variety of computing devices, including laptops and smartphones, across networks like the Internet.

Resource pooling involves providers offering cloud services to numerous clients while leveraging pooled computing resources. To separate and safeguard each customer's data from that of other customers and to give the impression to consumers that they are the only users of a shared computer or software application, virtualization and multi-tenancy methods are often utilized.

Rapid elasticity makes it possible to quickly and automatically raise and reduce the amount of processing, storage, and network bandwidth available in response to consumer demand

- **Pay-per-use measured service** entails allowing consumers to monitor their utilization and only pay for the computing resources that they actually utilize. This is comparable to how households utilize utilities like electricity.
- Remotely access anytime
- Scalability and flexibility high security and dependability.
- Now, businesses can dream large but start small with tight finances.

2. BACKGROUND AND RELATED WORK

2.1 Overview of business drivers to adopt cloud computing

Cloud computing offers organizations the opportunity to leverage advanced technologies such as virtualization and global Internet access. Some of the key business benefits include exploring new business opportunities, like experimenting with innovative ways to connect and engage with customers online.

By replacing upfront costs with predictable operational expenses and paying only for the computing processing and data storage that is actually used, organizations can reduce capital expenditures for computer equipment and related expenses, such as physical data centers and support staff. This reduces financial risk for the organization.

Shared infrastructure and technical expertise, often used by multiple customers to achieve economies of scale, could potentially lower ongoing costs. However, the cost of implementing security controls to address security risks, especially those associated with shared infrastructure, may offset some of the cost savings of certain types of cloud computing.

Guaranteed network connectivity for users allows the infrastructure to quickly scale up or down to meet fluctuating demand, and having computing infrastructure located in multiple physical locations improves disaster recovery. These factors could enhance business continuity and availability of computing infrastructure, while also potentially reducing carbon footprint due to more efficient hardware.

Transferring publicly accessible data to the public cloud can make commercial sense. Additional network bandwidth and processing power provided by vendors can automatically mitigate various types of distributed denial of service (DDoS) attacks on computer applications. This reduces financial waste caused by DDoS attacks. Technologies like "anycast" and global Content Delivery Networks (CDNs) help distribute network traffic and processing globally, improving availability and business continuity of publicly available data.

Confidentiality of data stored or processed using cloud computing may not be a concern, particularly for public websites. However, organizations should assess the accessibility and reliability of public data, as well as any reputational or other harm that could arise from corrupted or offline systems disseminating false information or malicious content.

Outsourcing specialized IT workers, computing software, and equipment for data storage and processing to vendors allows organizations to focus their internal resources on core operations. However, the organization remains responsible for ensuring the security of their data.

3. NEED AND IMPORTANCE OF RESEARCH PROBLEM

The ubiquity of cloud computing is undeniable. Every advancement and drawback in the as-a-service model makes headlines with equal fervor. Suppliers tout it as the solution to all business challenges and cost-cutting endeavors. IT professionals are hurrying to devise cloud strategies that not only save costs but also provide the operational agility needed to compete in the market. However, most organizations still use the cloud for only a fraction of their IT needs.

The "cloud" refers to remote servers accessed via the internet for corporate applications, add-ons, and software use. It allows PCs to connect to internet-based services and programs. Cloud computing enables access to various web services, sales force automation, office tools, blogs, spam filters, and data storage with a single login, saving money on multiple subscriptions. Businesses benefit from improved tracking and prevention of technological mishaps like data loss, viruses, and system crashes.

Storing vast amounts of business data on virtual servers enables seamless sharing among multiple offices. This web-based program doesn't require special equipment or servers; anyone traveling can access it via a virtual private network (VPN), reducing frustration and saving time. Cloud computing is not only a fantastic money-saving tool but also provides invaluable services in emergencies by enabling continuous monitoring of devices and applications. This ensures uninterrupted services and faster access to technology solutions, reducing business risks. Hosting firms offer innovative technological solutions that can significantly enhance organizations by tapping into various business opportunities.

4. OBJECTIVES

The objective focuses on technologies specific to the dimension of software and access to services and ownership. It will support long-term research on new principles, methods, tools and techniques enabling software developers in the EU to easily create interoperable services based on open standards, with sufficient flexibility and at a reasonable cost. Target outcomes

a) Cloud Computing

- Intelligent and autonomic management of cloud resources, ensuring agile elastic scalability. Scalable data management strategies, addressing the issues of heterogeneity, consistency, availability, privacy and supporting security.
- Technologies for infrastructure virtualization, cross platforms execution as needed for service composition across multiple, heterogeneous environments, autonomous management of hardware and software resources.
- Interoperability amongst different clouds, portability, protection of data in cloud environments, control of data distribution and latency.
- Seamless support of mobile, context-aware applications.
- Energy efficiency and sustainability for software and services on the cloud.
- Architectures and technologies supporting integration of computing and networking environments; implications of Cloud Computing paradigm on networks
- Open Source implementations of a software stack for Clouds

b) Internet of Services

- Service engineering principles, methods and tools supporting development for the Internet of Services, including languages and tools to model parallelism.
- Services enabled by technologies for seamless integration of real and virtual worlds, through the convergence with Internet of Things and Internet of Contents.
- Massive scalability, self-management, verification, validation and fault localization for software-based services.
- Methods and tools to manage life cycle of secure and resilient Internet-scale applications from requirements to run-time and their adaptive evolution over time.

c) Advanced software engineering

- Advanced engineering for software, architectures and front ends spanning across all abstraction levels.
- Quality measure and assurance techniques which adapt to changing requirements and contexts, to flexibly deal with the complexity and openness of the Future Internet.

d) Coordination and support actions

- Support for standardization and collaboration in software and services technologies.
- Support for the uptake of open source development models in Europe and beyond.
- Collaboration with Japanese entities on: cloud computing, particularly on common standards for data portability and on interoperability; services having more efficient energy usage.

5. SECURITY PROBLEM OF CLOUD COMPUTING

In cloud computing, resources are highly centralized, and the super-storage center on the Internet provides storage services for users by virtualization Technology. On the other hand, data owners care about their data, or reveal to the third party without authorization. The trust management between data owners and storage services providers is the essential problem in cloud security, which demands for an effective stipulation of data usage.

The proposed a data coloring method based on cloud watermarking to solve the trust management issue between data owners and storage service providers. Protecting datacenters must first secure cloud resources and uphold user privacy and data integrity. Trust overlay networks could be applied to build reputation systems for establishing the trust among interactive datacenters.

A watermarking technique is suggested to protect shared data objects and massively distributed softwaremodules. These techniques safeguard user authentication and tighten the data access-control in public clouds. The new approach could be more cost-effective than using the traditional encryption and firewalls to secure the clouds.

6. METHODOLOGY

Digital watermarking is a technology of copyright protection, which embeds the copyright information into digital production to avoid, being tampered, peculated, and illegally copied. The main idea of watermarking is to introduce small images or patterns into the data to be watermarked without affecting the data subject to normal use. If an illegal copy occurs, the owner of the data can therefore get watermarks from the illegal data to verify his ownership of the data. Cloud watermarking is a digital watermarking technology based on cloud model, which has widely been applied in text and relation database. Cloud model is a transform model between qualitative concepts and quantitative data. In this we firstly user have to create it's account in the cloud to access any cloud services here it's all data have been recorded in database, like image, it's login information, and other user necessary information. When ever user login to account it's entry recorded then after user upload the image in the cloud, here image is firstly checked weather the image is already available in the database if it is then it will be compared with existing image to get it's similarity factor and similarity percentage

In the process of data coloring, the location of the watermark to be embedded and the algorithm for embedding are decided by a user's requested security strength and allowable expense. Security strength will determine extra storage space, and algorithm complexity will decide time expense of data accessing.

At present, most of the watermarking algorithms focus on multimedia data, especially on digital images. The common digital watermark embedding algorithms include airspace algorithm, patchwork algorithm, Nippon electric company (NEC) algorithm, physiological model algorithm, etc. According to the different data source type (such as image, video, audio, and text), different embedding methods will be adopted. In our view, the colored data is also usable, so the watermarking changes the original data only with a subtler granularity. The granularity is decided by data source type. For a group climate data, in order to ensure the usability of data, we can embed watermarks by adding tails into data that only change the precision rather than the correctness.

6.1 Cloud model

To ensure that when the security features are stable, these features can be included by the algorithm that is embedding your image as a watermark, the preparation algorithm is merged with the creation of the protection features as well as the administration framework. The three characteristics worked together to create the objects' basis. The planning algorithm additionally provides the website link that is website the technical and administration aspects of the most wonderful solution is. When you look at the choice this is certainly first using the flow drawing (figure 4.2) a dedication with this standing in connection with image that is incoming created to cope with the problem of user watermarks passages supplier watermarks. To ensure that when the security features are stable, these features can be included by the algorithm that is embedding your image as a watermark, the preparation algorithm is merged with the creation of the protection features as well as the administration framework. The three characteristics worked together to create the objects' basis.

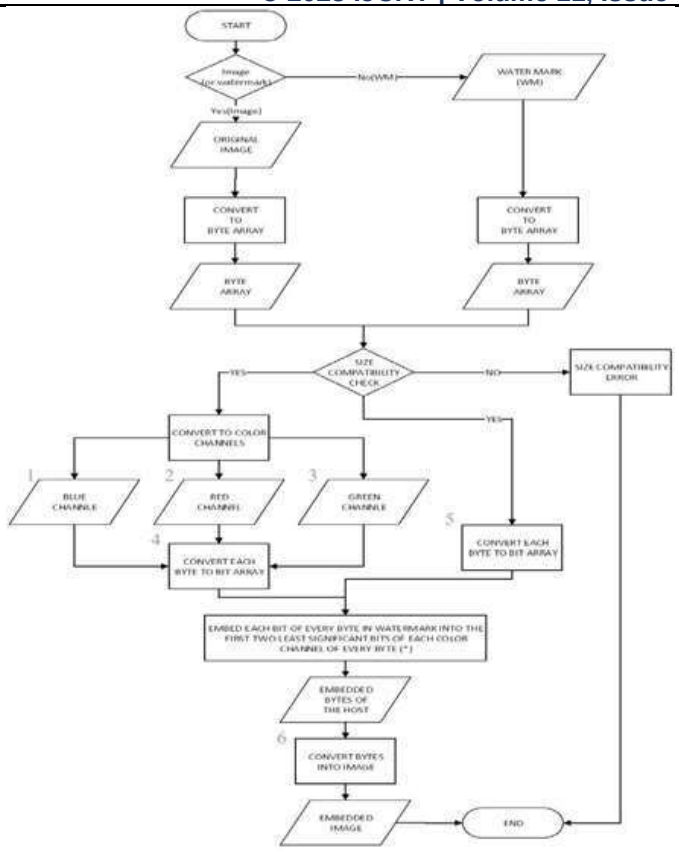

Figure : Flow Chart

6.2 Water marking using colour drop technique

Compare with pervious digital water marking technique, the colour drop water marking not just embed user copyright into data, but dynamic code of user data. That is to say not only the hole data is embedded with water marking but a fragment is branded. Each time, each user will get a random dynamic password for its data, which is able to protect copyright and should not affect the normal use of data. In the procedure of colour drop watermarking the image is converted into bit of array which is embedded with fix password, Dynamic password and HASH code using DWT embedded process which form invisible water marking image.

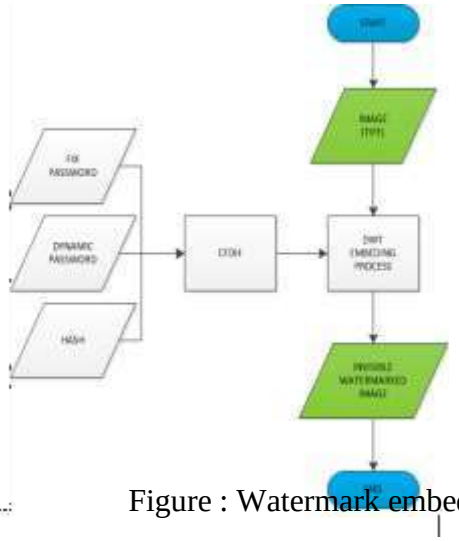

Figure : Watermark embedding

6.3 Colour drops

The colour drop Technique for invisible water marking a random password generator embedded with fix password which is converted into bit of array which again converted into hexadecimal code. The colour generator will generate the colour with the hexadecimal code which is used for water marking the location for water marking is randomly generated.

6.4 Water mark detection

For water marking the image, we are using user password and dynamic password which is randomly generated every time. In colour drop water marking technique a random location is selected for colour drop in such a way that it will not effect the data/information. Every time its SHA-512 and HASH code is generated. While removing the water marking these information(SHA-512(HASH), dynamic password, user pass word)is used.

These will provide high level of security and ownership detection to the user.

7. SCOPE OF WORK

The range decrease in this analysis's available data offers a lot of opportunities for further work. The implications of what has been accomplished go beyond what has already been done to address some of the several other open problems in the field of appropriate for ownership and digital rights. Following is a list of the essential points in each paragraph:

Future research growth may focus on various file types, which might be examined and tested for their suitability for employing the methodologies and watermarking described in this study.

According to the literature review for this thesis, little attention has been given to the persistent issues that cloud computing has brought up regarding the protection of intellectual property and privacy. There has to be a thorough investigation of this area as well as the effects of cloud computing as an information technology with regard to these issues.

Because of its utility, the model that has been created can now be transferred into different situations to test. The technology developed here has energy value because it may be installed in various locations where people are now using the cloud for information management. The wellness industry includes, for instance, the legal, educational, and training sectors.

The updating of cloud policies, particularly from the cloud service providers' end, including the security and privacy as well as other ownership issues, is one of numerous larger issues that has not been addressed. In order for lawmakers and other stakeholders in computer services to fairly explain settings that will benefit both the final user and the cloud provider, further research on this topic is necessary at the policy level.

The major challenge in this area is for consumers to be able to access practical applications online and for cloud providers to have access to them. In order to handle the biggest problems that are still unresolved, there needs to be computer software that is undoubtedly more aware of the problem. This thesis has made a contribution that is unquestionably significant, filling a vacuum not only in the literature but also in the practical application of services that could safeguard legitimate ownership and online rights.

9. CONCLUSION

Cloud security is a big concern as cloud computing grows. While using the cloud to handle security issues isn't new, viruses and software problems still exist on the internet. Cloud computing offers security services through specialized centers, but it's not just a technical problem like computer or network security. This study aims to offer new insights into cloud security by focusing on trust between data owners and service providers. We propose a method called data coloring based on cloud watermarking. Our experiment shows that this process is uncertain and irreversible, but a reliable reverse cloud generator can ensure users' social reputation identifiers. Despite the impact of cloud computing on daily activities like online shopping and working from home, many people are still unsure about its security. Like with reliability and safety, a service provider's reputation is important for trust, and cloud computing relies on this trust. In the future, we'll continue researching cloud computing, evaluating our method's effectiveness, and possibly creating a standard for cloud security.

REFERENCES

[1]. M. Miller. Cloud Computing: Web-based Applications That Change the Way You Work and Collaborate Online, USA: QUE, 2008.

[2]. Y. Zhang, D. N. Zhao, D. Y. Li. Watermarking relational databases. Journal of PLA University of Science and Technology, vol. 4, no. 5, pp. 1-4, 2003.(in Chinese)

[3]. E. Bertino. Data security. Data & Knowledge Engineering, vol. 25, no. 1-2, pp. 199-216, 1998. [4]. D. Y. Li, Y. Du. Artificial Intelligence with Uncertainty, New York, USA: CRC Pzess, 2007. [5]. C. Rey, D. Jean-Luc. A survey of watermarking algorithms for image authentication. EURASIP Journal on Applied Signal Processing, vol. 2002, no. 1, pp. 613-621, 2002.

[6]. D. Y. Li, X. M. Shi, H. J. Meng. Membership clouds and membership cloud generators. Computer Research and Development, vol. 32, no. 6, pp. 15-20, 1995. (in Chinese)

[7]. S. E. I. Baba, L. Z. Krikor, T. Arif, Z. Shaaban. Watermarking of digital images in frequency domain. International Journal of Automation and Computing, vol. 7, no. 1,pp. 17-22, 2010.

[8]. G. Lo-Varco, W. Puech, W. Dumas. Content based watermarking for securing color images. Journal of Imaging Science and Technology, vol. 49, no. 5, pp. 464-473, 2005.

[9]. X. Kong, R. Feng. Watermarking medical signals for telemedicine. IEEE Transactions on

Information Technology in Biomedicine, vol. 5, no. 3, pp. 195-201, 2001.
[10]. Z. H. Zhang, X. M. Jin, J. M. Wang, D. Y. Li. Watermarking relational database using image. In Proceedings of the 3rd International Conference on Machine Learning and Cybernetics, IEEE, Shanghai, PRC, vol. 3, pp. 1739-1744,2004.
[11]. R. Agrawal, J. Kiernan. Watermarking relational databases. In Proceedings of the 28th VLDB Conference, ACM, Hong Kong, PRC, pp. 155-166, 2002.