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. 3, Issue. 5, May 2014, pg.702 – 707

RESEARCH ARTICLE

Fingerprinting Based Recursive Information Hiding Strategy in Cloud Computing Environment

Varsha Yadav[1], Preeti Aggarwal[2]

[1]PG Student, Department of Computer Science & Engineering, KIIT College of Engineering, India

[2]Asst. Professor, Department of Computer Science & Engineering, KIIT College of Engineering, India

[1] vrshyadav91@gmail.com; [2] preetaggarwal@gmail.com

Abstract— The collection of interconnected servers that are provisioned dynamically on demand, for the execution of applications, to the customer is referred as cloud systems. Cloud computing provides clients the facility to store their data on the cloud; hence security of data stored on the servers of datacenters of Cloud service providers is an important issue. This paper proposed a scheme that helps in ensuring the security of data stored in the servers of Cloud systems. The proposed scheme is based on two methods – Information splitting and Fingerprinting. Information splitting helps in maintaining confidentiality and integrity of data and Fingerprinting helps in recovery of data. The property of proposed scheme that makes it different from existing data storage schemes is that integrity is ensured by client. This property may help in gaining trust of clients.

Keywords— Cloud computing; security; data storage; fingerprinting; confidentiality

I. INTRODUCTION

Cloud computing can be defined as a way of computing in which dynamically scalable and often virtualized resources are provided as a services over the internet. Internet is not only a communication medium but, because of the reliable, affordable and ubiquitous broadband access, is becoming a powerful computing platform rather than running software and managing data on the desktop computer or server, user are able to execute application and access data on demand from the cloud (internet) anywhere in the world [1]. In cloud computing model there are three service models and four deployment models which are explained below.

A. Types of Service Models in Cloud

The cloud computing service models [2] are discussed below as:

1) Software as a Service (SaaS): Under this layer, applications are delivered through the medium of the Internet as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management.

2) Platform-as-a-service (PaaS): To understand this cloud computing layer one needs to remember the traditional computing model where each application managed locally required hardware, an operating system, a database, middleware, Web servers, and other software. One also needs to remember the team of network, database, and system management experts that are needed to keep everything up and running. With cloud computing, these services are now provided remotely by cloud providers under this layer.

3) Infrastructure as a Service (IaaS): Products offered via this mode include the remote delivery (through the Internet) of a full computer infrastructure (e.g., virtual computers, servers, storage devices, etc.).

B. Deployment Models in Cloud computing

The four types of cloud [3] available in cloud computing are following:

1) Private cloud: The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.

2) Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community 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 on premise or off premise.

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.

4) Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

There are various issues in Cloud that is preventing organizations from using Cloud. One of these issues is security.

Security: While leading Cloud services providers employ data storage and transmission encryption, user authentication, and authorization (data access) practices, many people worry about the vulnerability of data to criminals like hackers, thieves, and disgruntled employees. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigating concern [4].There are many issues that are faced by cloud computing security.

The major issues faced by Cloud Computing Security are discussed below:

1) Insecure application programming interfaces: Cloud providers supply some kind of software interfaces for the customers, weak and user friendly interfaces exposes security issues [5].

2) Account, service and traffic hijacking: Stolen credentials used for this kind of attacks on the clouds which are usually taken by phishing, fraud or Denial of Services (DoS) [5].

3) Malicious Insider: A malicious insider is a person motivated to create a bad impact on the organization's mission by taking action that compromises information confidentiality, integrity, and/or availability. The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data and services with impact on the internal activities, organization's reputation and customer trust. This is especially important in the case of cloud computing due to the fact that cloud architectures require certain roles, like cloud administrators, cloud auditors, cloud security personnel, which are extremely high-risk. Cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The management of security risk involves users, the technology itself, the cloud service providers, and the legal aspects of the data and services being used. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective than traditional ones. To help reduce the threat, cloud computing stakeholders should invest in implementing security measures to ensure that the data is being kept secure and private throughout its lifecycle [6].

4) Data loss/leakage: Deletion or alteration of records without proper backups and loss of encoding key make the cloud difficult to restore. Unauthorized access into cloud can leads to data theft and losses [5].

Since cloud computing technology provides user the facility to store their data in the datacenters of cloud, security of data is an important concern. This paper proposed a scheme which helps in ensuring the security of data stored on the cloud. The proposed scheme is based on two methods – Information splitting and Fingerprinting. Information splitting helps in maintaining confidentiality and integrity of data and Fingerprinting helps in recovery of data. The property of proposed scheme that makes it different from existing data storage schemes is that integrity is ensured by client. This property may help in gaining trust of clients.

II. **LITERATURE REVIEW**

The Cloud computing [5] concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure and operational expenditure. In order for this to become reality, however, there are still some challenges to be solved. Most important among these are security and trust issues, since the user's data has to be released to the Cloud and thus leaves the protection sphere of the data owner. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. Security is to save data from danger and vulnerability. There are so many dangers and vulnerabilities to be handled. Various security issues and some of their solution are explained in this paper. This paper concentrates mainly on public cloud security issues and their solutions. Data should always be encrypted when stored (using separate symmetric encryption keys) and transmitted. If this is implemented appropriately, even if another tenant can access the data, all that will appear is gibberish. So a method is proposed such that the whole data is encrypted along with the cryptographic key.

In [7] author has given a brief introduction on Cloud computing and touched some of the security issues related to a cloud. Having explained the problems in the cloud, author has also proposed some solutions to the same with the help of algorithms like the DES and RAS Algorithms.

Cloud computing [8] 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.

Cloud computing [9] is the way of providing computing resources in the form of service rather than a product, utilities are provided to the users over internet. The main goal of cloud computing concept is to secure, protect the data and the processes which come under the property of users. The security of cloud computing environment is an exclusive research area which requires further development from both the academic and research communities. In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper digital signature method is proposed to protect the privacy and integrity of outsourced data in cloud environment. This paper used RSA algorithm for digital signature and for the process of encryption and decryption.

Increasing demand for cloud applications [10] has led to an ever growing need for security mechanisms. The most serious concerns are the possibility of lack of confidentiality, integrity and authentication among the cloud users and service providers. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication. In this paper symmetric and asymmetric cryptographic algorithms are adopted for the optimization of data security in cloud computing.

In [11] the problem of ensuring the integrity of data storage in Cloud Computing is studied. In particular, they have considered the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. The authors first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in their protocol design. In particular, to achieve efficient data dynamics, they improve the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, they further explore the technique of bilinear aggregate signature to extend the main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

With the advent of the World Wide Web **[**12**]** and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. This data would be more useful to cooperating organizations if they were able to share their data. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. In this paper these issues are addressed by combining cloud computing technologies such as Hive and Hadoop with XACML policy based security mechanisms that provide fine-grained access to resources. This paper further presents a web-based application that uses this combination and allows collaborating organizations to securely store and retrieve large amounts of data.

A k-out-of-n recursive information hiding scheme based on an n-ary tree data structure is described in [13]. In recursive hiding of information, the user encodes additional information in the shares of the secret intended to be originally shared, without an expansion in the size of the latter. The proposed scheme has applications in secure distributed storage and information dispersal protocols. It may be used as a steganographic channel to transmit hidden information, which may be used for authentication and verification of shares and the reconstructed secret itself.

The scheme proposed in [3] is introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

A recursive computational multi secret sharing technique is presented in [14] that hides k - 2 secrets of size b each into n shares of a single secret S of size b, such that any k of the n shares suffice to recreate the secret S as well as all the hidden secrets. This may act as a steganographic channel to transmit hidden information or used for authentication and verification of shares and the secret itself. Further, such a recursive technique may be used as a computational secret sharing technique that has potential applications in secure and reliable storage of information on the Web, in sensor networks and information dispersal schemes. The presented technique, unlike previous computational techniques, does not require the use of any encryption key or storage of public information.

III. **PRESENT WORK**

The security of data stored on the severs of cloud is an important issue in cloud computing technology. In the present work a scheme is proposed which helps in ensuring the security of data stored on the cloud. The proposed scheme is based on two methods – Information splitting and Fingerprinting. Information splitting helps in maintaining confidentiality and integrity of data and Fingerprinting helps in recovery of data. Since the fingerprints have zero collision property, only the original user can access or modify the data. This property may help in gaining trust of clients. The property of proposed scheme that makes it different from existing data storage schemes is that integrity is ensured by client. The steps followed in the proposed scheme are as follows:

- In the first step, File is taken from the client.
- In second step, for ensuring data storage security, processing of data takes place. This includes splitting of file into shares and then Fingerprinting of shares is performed in the third step.
- In fourth step, shares of the file are sent to different servers. The information about which share is sent to which server is stored in the cloud monitor.
- In order to reconstruct the file, user enters the file name and fingerprint from any client system. These details are searched from the cloud monitor.
- On comparison if it is determined that fingerprint doesn’t match then the shares are not integrated.
- If the fingerprint matched with the one that was used at the time of storing the file on cloud then only the shares get integrated and the file will be retrieved.

Cloud monitor that is used in the proposed scheme is a server whose task is to keep track of which share is stored on which server in the cloud. The steps followed in the proposed scheme are explained as follows:

After sending the file to the Cloud service provider, file is recursively divided into shares using information splitting scheme. In information splitting scheme, shares are created as follows: size of each share is taken as 200 bytes. Then number of shares (k) is calculated as k= (Size of file)/200). If still some characters left then one more share is created i.e. k=((size of file)/200+1). After dividing the file into shares, encryption of shares is performed using AES algorithm. The key used for encryption is the key corresponding to the client’s fingerprint and this key is generated using RSA algorithm. These encrypted shares are then stored on the servers. The details like servers' ip addresses and names of the shares with their respective fingerprint's key are stored in cloud monitor. This adds security to the shares. If anyone attempts to attack the shares of the file, then fingerprint of the client/sender will be required. The fingerprint is then sent to client who is part of the group among which this file has to be shared.

When the client wants to retrieve the file from the cloud he/she will give the name of the file and the respective fingerprint. The given fingerprint's key is then generated. These details are searched from the cloud monitor. If the fingerprint key matched with the key that is used for encrypting the shares of the file at the time of storing the file on the cloud, then the shares get decrypted using this same key and these decrypted shares get integrated and the file will be retrieved. In case the fingerprint does not match with the one whose key is used at the time of storing the file on cloud then the file will not be retrieved.

A. FLOWCHARTS OF THE PRESENT WORK

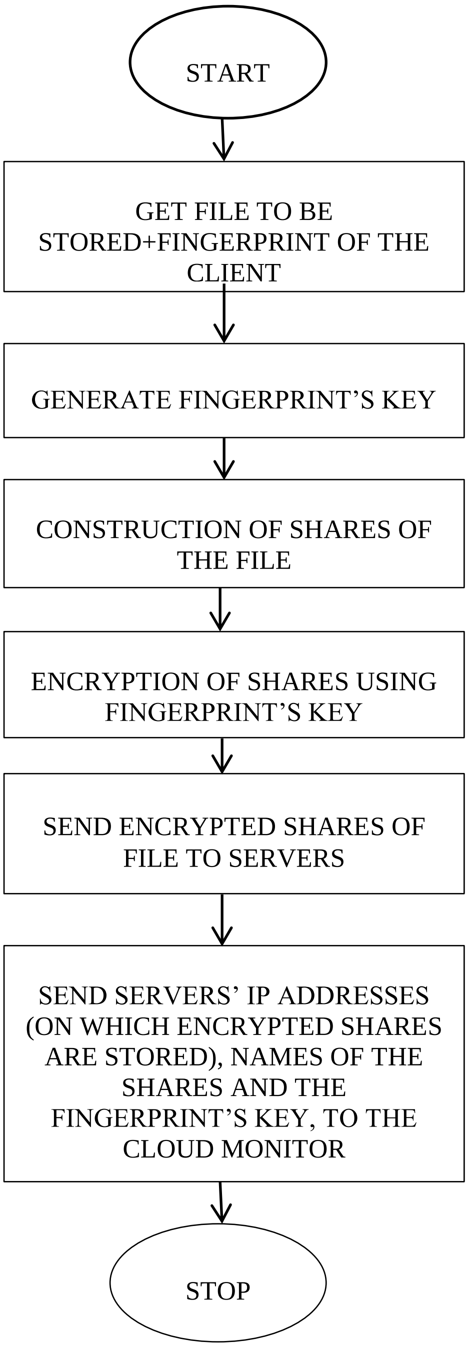
START
GET FILE TO BE STORED+FINGERPRINT OF THE CLIENT
GENERATE FINGERPRINT'S KEY
CONSTRUCTION OF SHARES OF THE FILE
ENCRYPTION OF SHARES USING FINGERPRINT'S KEY
SEND ENCRYPTED SHARES OF FILE TO SERVERS
SEND SERVERS' IP ADDRESSES (ON WHICH ENCRYPTED SHARES ARE STORED), NAMES OF THE SHARES AND THE FINGERPRINT'S KEY, TO THE CLOUD MONITOR
STOP

Fig. 1 Flowchart for data storage

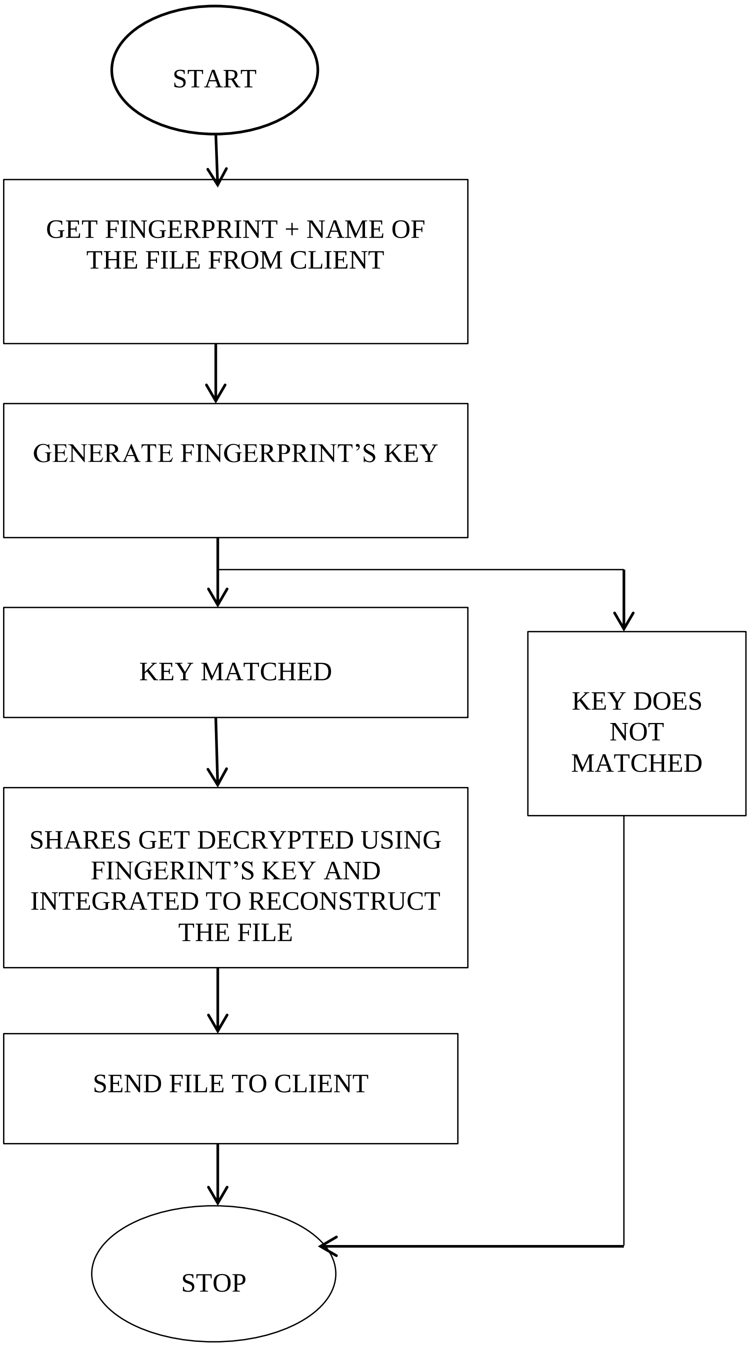
START
GET FINGERPRINT + NAME OF THE FILE FROM CLIENT
GENERATE FINGERPRINT'S KEY
KEY MATCHED
KEY DOES NOT MATCHED
SHARES GET DECRYPTED USING FINGERINT'S KEY AND INTEGRATED TO RECONSTRUCT THE FILE
SEND FILE TO CLIENT
STOP

Fig. 2 Flowchart for data retrieval

IV. **RESULT**

The proposed scheme is implemented in java and simulation is done using CloudSim tool. The performance of the proposed scheme is high as it satisfactorily meets the parameters of security i.e. confidentiality, integrity and recovery. By meeting these parameters, proposed scheme ensures data security.

V. **CONCLUSION**

In this paper a methodology is proposed for ensuring the security of data stored on the servers of cloud systems. In the proposed scheme, instead of storing the file on the single server, encrypted shares of the file are stored on different servers, and key used for encryption and decryption is the fingerprint's key of the sender and since the fingerprints have zero collision property this method ensures the security of data stored on the servers of the cloud. This scheme is best suited for those Cloud service providers where main focus is to give secured data storage services and space is not a problem.

In this paper, only one secret file from the client is securely stored. In future this scheme can be used for storing multiple files from the same client. This scheme may also be used in army for sending confidential information.

ACKNOWLEDGEMENT

I would like to thank almighty and my family for their constant support during this work. I would also like to thank my professor Ms. Preeti Aggarwal for her guidance and valuable support during this work.

REFERENCES

[1] S. Sharma, S. Soni and S. Sengar, "Security in cloud computing," in *Proc. National Conference on Security Issues in Network Technologies,* Aug. 2012.

[2] N. Sultan, "Cloud computing for education: A new dawn?," *International Journal of Information Management,*2010.

[3] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, 2012.

[4] (2010) DataPlex.com/blog/ [Online]. Available: http://www.dataplex.com/blog/index.php/2010/01/07/Cloud-computing-issues/

[5] G. Thomas, P.J.V. and P.Afsar, " Cloud computing security using encryption technique," *IJASCSE*, 2013.

[6] F. O. Neamtiu, "Cloud computing security issues," *Journal of Defense Resources Management,* 2012.

[7] V. Alangar, "Cloud computing security and encryption," *International Journal of Advance Research in Computer Science and Management Studies,* Oct. 2013.

[8] N. Singh and S. Singh, "The amalgamation of digital watermarking and cloud watermarking for security enhancement in cloud computing," *International Journal of Computer Science and Mobile Computing,* Apr. 2013.

[9] K. Govinda, V. Gurunathaprasad and H. Sathishkumar, "Third party auditing for secure data storage in cloud through digital signature using RSA," *International Journal Of Advanced Scientific and Technical Research,* Aug. 2012.

[10] M. Sudha and M. Monica, "Enhanced security framework to ensure data security in cloud computing using cryptography, "*Advances in Computer Science and its Applications,* Mar. 2012.

[11] Q. Wang C. Wang, K. Ren, W. Lou and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel And Distributed Systems,* May 2011.

[12] V. Khadilkar, A. Gupta, M. Kantarcioglu, L. Khan and B. Thuraisingham, "Secure data storage and retrieval in the cloud," in *Proc. 6th International Conference on Collaborative Computing,* 2010.

[13] A. Parakh and S. Kak, "A tree based recursive information hiding scheme," in *Proc. IEEE International Conference on Communications (ICC),* 2010.

[14] A. Parakh and S. Kak, "Recursive secret sharing for distributed storage and information hiding," in *Proc. IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems,* 2009.