ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 4, APRIL 2015, PP 260-263

An Intensify approach of Data owner Dominant Model for Safeguard Data security in Cloud

Maninder Singh Bajwa, Himani

Abstract— Cloud computing is the innovative trendy technology which diversified their role in whole world business but demerits of cloud become an obstacle to opt this technology, So frequent enhancements are required to make this technology worthy. The vital concerns are data security, data privacy, data leakage, integrity and data confidentiality due to which this mechanization lacks behind. To solve these problems we proposed a model which intensifies data security and is based on data owner dominance. Encryption, Obfuscation, HMAC and Dual authentication and access management techniques have been used which make this model trustworthy and efficient for usage.

Index Terms— Cloud Computing, Data Owner Dominant, Data Security, Hash Code, Encryption, Obfuscation.

1 INTRODUCTION

CLOUD Computing set up pervasive, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be immediately provision and released with essential efforts for management or service provider interaction. Its main objective is to deliver quick, secure, convenient data storage and net computing service, with all computing resources envision as services and delivered over the Internet.

A number of computing concepts and technologies are combined in Cloud Computing to satisfy the computing needs of users, it provides common business applications online through web browsers, while their data and software's are stored on the servers. This is an approach that is used to maximize the scope or step up capabilities robustly without investing in new infrastructure, sustenance new personnel or licensing new software. It provides tremendous storage for data and rapid computing to customers over the internet.

Data security is one of the aspects of the cloud which prohibit users from using cloud services. There is fear between the data owner's especially in large organizations that their data possibly misuse by the cloud provider without their knowledge. Data security of the user's can be ensured by using the concept of virtual private networks, firewalls, and by enforcing other security policies within its own circumferences. Security is consequently an extensive element in any cloud computing environment, because it is crucial to assure that only authorized access is sanctioned and protected behaviour is accepted.

Any kind of security and privacy contravention is critical and can produce crucial results. As soon as the strict regulations and policies are taken against privacy in cloud, more and more personnel will feel save to adopt cloud computing. A client may be individual or a big organization but all are having same concern i.e. data security, so data security is dire consequence. Data security at different levels is the vital matter of this technology; it can be categorized into two categories: Security at External level and Security at Internal Level. Security at External level states that data is unsecure opposed to third party, cloud service provider or network intruder. Security at Internal level states that data is unsecure opposed to authorized users or employee of an organization.

Section II discusses the related work done in the field of data security in cloud. Section III describes the gaps in existing literature. Section IV desirable the proposed model Section V we conclude with our work.

2 RELATED WORK

There are numerous work carried in the field of data protection at cloud. Many models, schemes and techniques are proposed for data security.

M. Sugumaran et al [10] illustrates a couple of techniques that resolves the security of the data and proposes architecture to safeguard the data in cloud. In proposed architecture the encrypted data is stored in cloud using cryptography technique i.e. located on block cipher. Cindhamani.J et al [3] proposed an enhanced frame work for data security in cloud which follows the security polices such as integrity, confidentiality and availability. Parameters they used are 128 bit encryption, RSA algorithm and Trusted Party Auditor (TPA). Before storing the data into the cloud, the data owner assigns the privileges that who will access the data. After

- ***Maninder Singh Bajwa*** *is pursuing M.Tech in Computer Science & Engineering in GIMET, Amritsar, Punjab, India.*
  E-mail: maninderbajwa90@gmail.com
- ***Himani*** *is working as Asst. Prof. in Department of Computer Science & Engineering in GIMET, Amritsar, Punjab, India.*
  E-mail: global.himani26@mail.com

ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 4, APRIL 2015, PP 260-263

assigning the privileges they encrypt the data and stores into the cloud. Dharmendra [4] proposed the unified data encryption architecture which ensures the data security and privacy with reasonable performance overhead of computing system. It is based on multilevel identity encryption approach with two level/factor identity verification process. Dr. L. Arockiam et al [5] achieves the data confidentiality in cloud storage with two different techniques i.e. encryption and obfuscation. Encryption encrypts the alpha-numeric and alpha data while obfuscation encrypts the numeric data. Both are done on user side. First, the user has to encrypt the data using any technique then he stores the data into cloud storage. Taeho Jung et al [14] use two schemes to control the data privacy and the identity privacy. One is the AnonyControl scheme i.e. semianonymous privilege control scheme which not only addresses the data privacy but also the user identity privacy in extant access control schemes. It decentralizes the central authority to restraint the identity leakage and thus achieves semianonymity. Another is the Anony-Control-F scheme that controls the identity leakage and achieves the full anonymity. Eman M.Mohamed et al [6] Exhibits the data security model that is based on the analysis of cloud architecture and implemented software to intensify endeavor in data security model for cloud computing. Hu Shuijing [7] described the enormous essentials in cloud computing, such as security key technology, regulation and standard etc and discussed manner in which they are addressed.

In this Proposed model data is protected against all threats i.e. internal and external, thread during, transits as well as when data at rest.

3 Gaps in Existing Literature

The gaps that exit in the literature of the dissertation are:

- Focus on data security but not able to provide full security at different levels.
- There are some questions which are unanswered such as Is data at cloud is in secure hand, during transit data is secure and if any third party is involved then can we trust that party.
- There are numerous techniques, models and schemes have been proposed in this field of data security but still some more enhancements are required so that data owner feel free to use cloud.

4 Proposed Model

In proposed model, data security at cloud is the main responsibility of the data owner as he is the only person who can handle the data more securely than any of the organization. For data security; encryption and obfuscation techniques are used to protect the data while transits as well as at rest. During traversing of data, Data integrity plays crucial role hence for data integrity hash based message authentication is used. To overcome the load of data owner the concept of third party is evolved.

The proposed model is divided into two categories i.e.

Case-1(uploading)

Case-2(downloading)

And involved four entities i.e. - data owner, CSP, third party and user.

4.1 Case -1 (Uploading)

4.1.1 Key Generation and maintenance

For key generation and storage the third party acts as a key management infrastructure. The third party generates the keys and handover these keys to the data owner for further processes. Data owner splits the key into two parts, in which he uses the one part for encryption and other for corresponding user verification. Before sending these keys back to third party for management, the data owner encrypts these two keys by passcode. Third party kept these key pieces and is taken from whenever required.

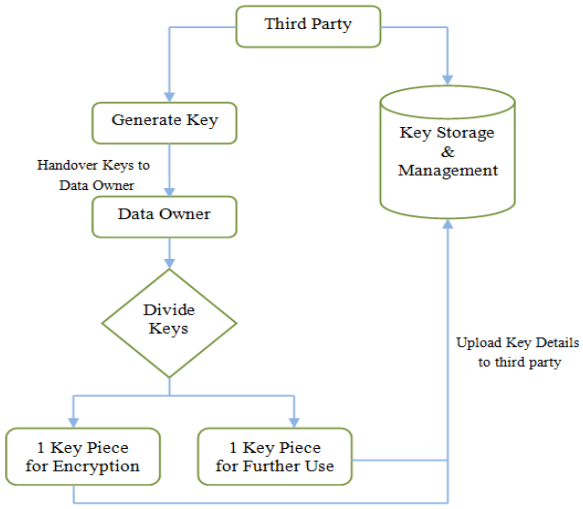

Figure 3.1. Key Generation and maintenance

4.1.2 Classification of data

The data can be classified into two types i.e. type 0 and type 1

Type 1:- when the classified data is of alpha numeric type.

Type 0:- when the classified data is of numeric type.

4.1.3 Encipher and Indexing

On the basis of classified data, corresponding encipher technique is used. The type of data is identified by the data owner itself. Encryption is taken place when the data is classified 1 otherwise obfuscation is performed. Before encipher techniques, indexing is performed. Thereafter the data is uploaded to cloud.

ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 4, APRIL 2015, PP 260-263

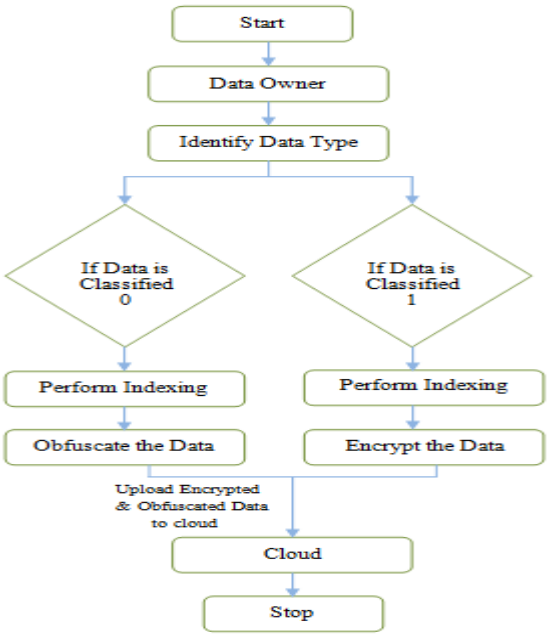

Figure 3.2 Encipher and Indexing

4.2.4 Data Integrity

Before uploading the data to cloud, hash based message authentication code (HMAC) is generated in order to check data privacy during traversing of data to cloud. In the same way as data is encrypted, HMAC is also encrypted after it is generated and uploaded to cloud.

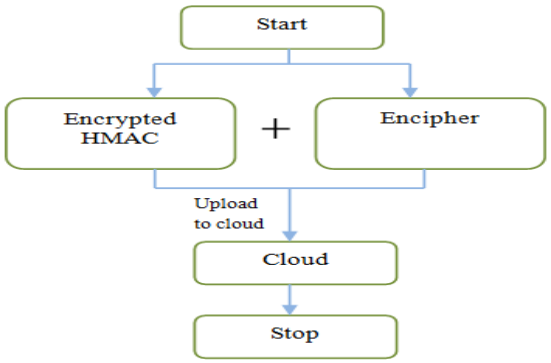

Figure 3.3. HMAC Generation for Data Integrity

4.2 Case 2: Downloading

4.2.1 Dual Authentication and Access Management:-

In this proposed model, dual verification exists so the data is secured against unauthorized user. Here the data owner shares its user database with cloud. Authenticated user login to cloud and get role base access to data. First data owner verifies the user with digital signature and passes the user id details to third party. Then, third party verifies the user id and handover the corresponding key piece to user. After getting the key the user will be able to decrypt the data.

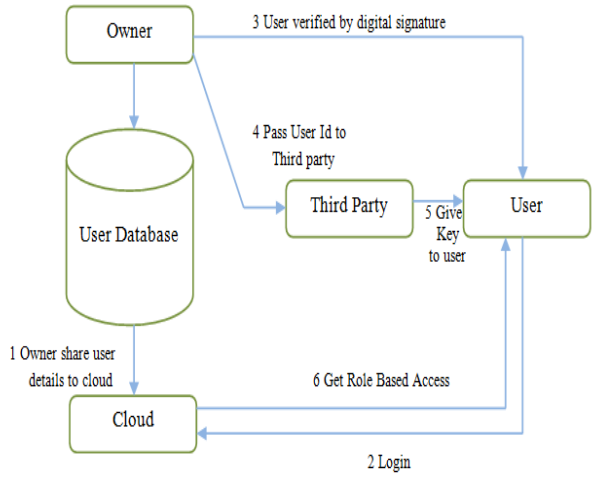

Figure 3.4 Dual User Authentication

4.2.2 HMAC verification

HMAC is used to check the data integrity and for this it is regenerated by the user and matched with original HMAC produced before the data is uploaded to cloud i.e.

HMAC (Uploading) =HMAC (downloading)

If both HMAC are not same then user has to report to data owner and if same then data is not tempered.

5 Conclusion & Future Scope

A prevailing trend shows that data security is an extensive aspect of cloud which prohibits users from using cloud services. There is fear between the users and data owner's especially in large organizations that there may be a possibility of data misuse by the cloud provider without their knowledge and hence, they hesitate to adopt this technology. To resolve this problem a model has been proposed which intensifies data security. It gives assurance that their data is secure during transit as well as at rest. It also assists the users to fearlessly upload the data at cloud without being any uncertainty that their data might be lost or stolen.

In future we implement this model to realistic project to make this model trustworthy and efficient for usage. Further, more parameters can also be added for enhancement.

References

[1] Ayad F. Barsoum et al "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 3, MARCH 2015.

[2] Chang Liu et. al. "MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud", IEEE TRANSACTIONS ON COMPUTERS.
[3] Cindhamani.J et al "An enhanced data security and trust management enabled framework for cloud computing systems", 5th ICCCNT – 2014.
[4] Dharmendra S. Raghuwanshi "MS2: Practical Data Privacy and Security Framework for Data at Rest in Cloud", 2014 IEEE.
[5] Dr. L. Arockiam et al "Efficient Cloud Storage Confidentiality to Ensure Data Security", 2014 International Conference on Computer Communication and Informatics, ICCCI -2014.
[6] Eman M.Mohamed et al "Enhanced Data Security Model for Cloud Computing", The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May, Cloud and Mobile Computing Track.
[7] Hu Shuijing "Data security: the challenges of cloud computing", 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation.
[8] Jingwei Li et.al. "Secure Auditing and Deduplicating Data in Cloud", 2015 IEEE Transactions on Computers.
[9] LiMa et. al. "Chances and Challenges Confronting Securities Industry and the Countermeasures in Big Data and Cloud Computing Era", ICCSE 2014.
[10] M. Sugumaran et.al. "An Architecture for Data Security in Cloud Computing", 2014 World Congress on Computing and Communication Technologies.
[11] Mazhar Ali et al "SeDaSC: Secure Data Sharing in Clouds", IEEE SYSTEMS JOURNAL 2015.
[12] Neelu Sinha et.al. "Cloud Computing Security, Data, And Performance Issues", WOCC 2014.
[13] Sandha et.al. "Study on Data Security Mechanism in Cloud Computing", 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14.
[14] Taeho Jung et. al "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.
[15] Tao Jiang et al "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", 10.1109/TC.2015.2389955, IEEE Transactions on Computers.