International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 9 (September'2017)

A STUDY ON SECURITY OF DATA STORAGE IN CLOUD COMPUTING

M. Madhunika,
Department of Computer Science,
Rajah Serfoji Govt. College,
Thanjavur, Tamilnadu,India.

R. Uma,
PG & Research Department of Computer Science,
Sri A.V.V.M. Pushpam College,
Poondi, Tamilnadu,India.

J.Gnana Jayanthi,
Department of Computer Science,
Rajah Serfoji Govt. College,
Thanjavur, Tamilnadu,India.

Abstract: Cloud computing is very fast grownup field and facing many technological advances in the recent era. It supply cost efficient architecture that support the transmission storage and intensive computing. Cloud is kind of Centralized database where many organizations store their data, retrieve data and possibly modify data. In the cloud many Services are provided to the client by cloud. Data store is main future that cloud service provides to the big organization to store huge amount of data. But still many organizations are not ready to implement cloud computing technology because of following reason. That is Lack of security, Data redundancy, Misbehavior of the server. So the main objective of this paper is to solve the above reasons that are To prevent unauthorized access, it can be done with the help of a distributed scheme by using homomorphism token to provide security of the data in cloud. The cloud is support for data redundancy means clients can insert, delete or can update data so there should be security mechanism which ensure integrity of data.

Key words: Cloud data Security, data Integrity, Cloud Providers, Cloud users

I.INTRODUCTION

Cloud computing is a new revolutionary technology it gives a high reliable services of digital content. The digital universe will grow by a factor of up to 40 trillion gigabytes of redundant data by 2020 the above factor declared by the US International Data Corporation (IDC). This rapid development of the digital Universe need more new storage space and network services and also need more cost effective for Data transfer.[1][2] The usage of Remote storage has achieved by the cloud storage based services it gives a high profitable architecture that support the transmission, Data storage and computational out sourced data in a pay per use of this model. Cloud storage services mainly used in business organization and government agencies to utilize the software as a service it gives the cost effective system instead of purchasing new software they just access the service and resources of the cloud. The delivery of the service in the cloud becomes very responsive, effective and efficiency. There is no need to buy any new software and hardware by spending the large amount of capitals instead of that the companies can use the service of the cloud storage.

All the above features bring some of the specific issues like security specifically in the data Communication and outsourcing. So the Cloud security is the essential problem raises in many aspects regarding the privacy of user to protect their outsource out source infrastructure increases their vulnerability to security incidents and attacks while moving the data client and the cloud server can done without the complexity due to the online base computing it provide the large amount of data storage and resources to the local machine and face the maintenance and hardware problem overcome by the cloud service providers for their availability and integrity of their data storage [1][2].

The quality of service need to addressed and overcome by the challenges with belongs to security and privacy in a cloud data storage instead of using a traditional services or networks that the cloud computing can provide the dynamic delivery of data on demand. It is highly deliver three types of services such as:

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Economically the above services they provide many attractions to the cloud users that the user can use only what they need and pay for that service only and it give ubiquitous service to all type users through the cloud network the user of the Cloud need not worry about the maintenance of the cloud service. To face the new challenges of the security threats to enhance the quality of service the traditional security in cloud computing. Cryptography cannot be used for data security many other new technique and algorithms used into protect data from the unauthorized user and malicious user and also new approaches used for to ensure the data integrity. The verification of the cloud storage must ensure the correctness without the explicit knowledge of the entire data [3].

II.FEATURES OF CLOUD DATA STORAGE

The core concept of the cloud technology extract from the US National Institute of standards of technology (NIST) of five aspects .The characteristics of the aspects of presented as follows

On Demand self Service: The Cloud user may access some extra resources such as usage of stored data and performance of the service and also server time and storage of networks as needed automatically without requiring the human interaction with its service provider this process is similar to automatic computing refer to the property of managing the characteristics of distributed computing resources and also reduce the barriers of the complexity raises.

Broad network Access: The variety of heterogeneous of thin or thick client platforms (such as mobile phones, tablets, laptops and other workstations and all hand held devices) has access the available service through the network and accessed the cloud service through the standard mechanisms. The Cloud provides the ubiquitous services using the standard protocol via the internet. All the public networks are untrusted by the several attacks like (MITM) man in the middle attacks.

Resource Pooling: The Resources of the Service Providers are shared among multiple users using a multi tenant model thereis no resource dedicated to specific clients but with the various physical and virtual resources are dynamically assigned and reassigned according to the demand and request of the users . The location independence of the customer generally has no control or knowledge over the exact location of the provided services also able to specify at high level of abstraction (eg Country, state or datacenter) The Resources including storage, processing memory and network bandwidth.

Rapid Elasticity: Capabilities can be elastically provisioned and released with efficiently. The properly demonstrate a scalability of greater resources. In such cases these resources are abstracted to cloud users in order to appear as unlimited and suitable services under provisioning of the bandwidth the malicious users can take advantage of a tarOct 2017get service or application availability through the denial of service attacks. Therefore the scalability and reliability is the important key factors of the elasticity of characteristic of a cloud models.

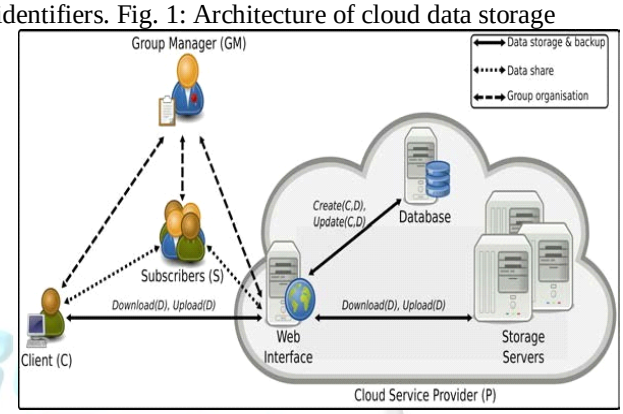
Measured Service: The service and resource usage can be explicitly viewed and monitored controlled and reported to the cloud providers and users. The following Process such as Storage, processing bandwidth and active user accounts can be metering the capability at some level of abstraction appropriate to the type of service. In this cloud based services the user pay only the consumption basis enabling major cost reduction. The above attributes of the cloud based system has compared to the traditional computing model supporting more efficient and scalable cloud system can be classified based on the deployment of Private, Public or hybrid infrastructure[4][5].

III.CLOUD STORAGE ARCHITECTURE

In this section, a typical cloud storage architecture. It relies on the following entities for the good management of a client data: · Cloud Service Provider (CSP): a CSP has significant resources to govern distributed cloud storage servers and to manage its database servers. It also provides virtual infrastructure to host application services. These services can be used by the client to manage his data stored in the cloud servers. ·

Client: a client makes use of provider's resources to store, retrieve and share data with multiple users. A client can be either an individual or an enterprise. ·

Users: the users are able to access the content stored in the cloud, depending on their access rights which are authorizations granted by the client, like the rights to read, write or re-store the modified data in the cloud. These access rights serve to specify several groups of users. Each group is characterized by an identifier IDG and a set of access rights. In practice, the CSP provides a web interface for the client to store data into a set of cloud servers, which are running in a cooperated and distributed manner[4][5]. In addition, the web interface is used by the users to retrieve, modify and re-store data from the cloud, depending on their access rights. Moreover, the CSP relies on database servers to map clients identities to their stored data identifiers and groups identifiers. Fig. 1: Architecture of cloud data storage



IV.CRYPTOGRAPHY IN CLOUD DATA STORAGE ENVIRONMENT

Cloud storage can evolved in a new trend of the computing field to provide the external Service to the users. This cryptography framework can protects the data security and privacy security management of this cloud computing performed by authorizing the signature of the different data involved in every element[6]. The data security and privacy concerns are latest evolutionary process of handling data storage at cloud. In November 2013 the Washington's post points more incriminate data structure and capture by the NSA this collection is done by Google and Yahoo data centers around the world and decrypting the traffic that protected in transmit there are many security concerns used in cloud computing the outsourcing encrypted data and periodically checking data integrity mechanisms used.

Symmetric Cryptography : Symmetric or conventional cryptography in this only one key used to encrypt and decrypt the data between the two common devices In Asymmetric cryptography the encryption where 2 keys private and public key are used for data confidentiality, non repudiation and authentication while exchange the information over an insecure channel. In symmetric cryptography where two communicating entities share the same key but in the asymmetric cryptography pair of keys used one is public and another is private key therefore the public key used for encryption and private for decryption.

Diffie Hellman Algorithms : This mechanisms mainly used to secure the internet services, It can Secure encrypted communication between two parties required that they first exchange keys by some secure physical channel, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher[6].

Elliptic Curve Cryptography (ECC) : Elliptic Curve Cryptography (ECC) was discovered in 1985 by VictorMiller (IBM) and NeilKoblitz (University of Washington) as analternative mechanism for implementing publickey cryptography. ECC algorithms rely on the algebraic structure of elliptic curves over finitefields. ECCis an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptograph.

IV.ID-BASED CRYPTOGRAPHY FOR SECURE CLOUD DATA STORAGE

Cloud user facing many difficulties of storing and maintaining a local storage infrastructure such cases the user can move the data to the cloud very securely and also they pair only the resources. The provider offer to the client to store retrieve and offer the resources to the client the security issues of the cloud data storage as overcome by the encrypting the out sourced data however the confidentially become more confidentiality provisioning becomes more complicated with flexible data sharing among a group of users[7][8]. It requires efficient sharing of decrypting keys between different authorized users. As such, only authorized users are able to obtain the clear text of data stored in the cloud.

ID-Based Cryptography (IBC) was initially introduced by Shamir to provide entities with public and private key pairs with no need for certificates. Shamir assumes that each entity uses one of its identifiers as its public key. These identifiers have to be unique. The private key generation function to a special entity called the Public Key Generator (PKG). That is, before accessing the network, every entity has to contact the PKG to get its private key. This private key is computed so as to be bound to the public key of the entity. During the last decade, IBC has been enhanced by the use of the Elliptic Curve Cryptography (ECC)[7][8]. As a consequence, new ID-based encryption and signature schemes emerged. In order to be able to derive a client's private key, the PKG must first define a set of ID-based public elements (IBC–PE). The PKG generates the groups G1, G2 and GT and the pairing function e^ from G1 × G2 in G .G1 and G2 are additive subgroups of the group of points of an Elliptic Curve (EC). However, GT is a multiplicative subgroup of a finite field. G1, G2 and GT have the same order q.

Application security on cloud: ID-Based Cryptography propose a many light weightkey management algorithm which provide own ID-Based Cryptography Public Elements (IBC-PE) to encrypt the data before their storage sharing in the cloud the computation of public keys from the unique data identifiers does not require the deployment of a Public Key Infrastructure (PKI) and the distribution of certificates with no need for previous computation of corresponding private keys any user can directly encipher data for a client at no extra cost of communication [9] . Privacy is a critical concern with regards to cloud storage due to the fact that clients' data reside among distributed public servers. Sensitive information are included in meta-data (e.g., file name, client identity, keywords)].First, meta-data content can never be disclosed to the CSP, as he only has access to hashed information $ID_D = H(MD)$. Second, the CSP cannot reveal the content of stored data. In fact, although, he has the data identifier and the public elements of the client IBC–PEC , he does not have the secret sC needed to derive the privatekeyanddecipherdata.Furthermore, searching for stored data, for a backup process, may also endanger the privacy.However, the enforcement of these propositions partially violates privacy protection, since the CSP can guess the content of the stored data based on keywords. To overcome this privacy problem, we propose to use the *hashed* meta-data as a data identifier is used. This identifier is unique and it will serve to search data from cloud servers.

Security Requirements: The design of a remote data checking scheme is motivated by providing support of both robustnessandefficiency,whileconsideringthelimitedstorageandprocessingresourcesof userdevices.Zero knowledge PDP protocol that provides deterministic integrity verification guarantees, relying on the uniqueness of the Euclidean Division presenting probabilistic approaches[10].

V.CONCLUSIONS

The growing need for secure cloud data storage services and the attractive properties of ID-based cryptography show the way us to. Defining an innovative solution to the data outsourcing security issue. Our solution is based on a specific usage of IBC..Finally, we believe that cloud data storage security is still full of challenges and of paramount importance, and many research problems remain to be identified. This research paper propose To study the efficient cryptographic mechanisms, in order to ensure data security in cloud data storage environments and also provide the suggestions of data confidentiality in cloud applications, while enhancing dynamic sharing between user In response to this objective, two different approaches are presented based on the usage of ID-Based Cryptography(IBC)and the convergent cryptography, respectively. Cloud storage clients are assigned the IBC–PKG function, where a per data key is derived locally from a data identifier and the data identity this mechanism is shown to support data privacy and confidentiality, as it

employs an original ID-based client side encryption approach.

VI.REFERENCES

[1]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song. Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, New York, NY, USA, 2007.ACM.

[2]. Nikita Pathrabe, Deepali lehatawar-"Ensuring Data storage in cloud computing "International Journal of Research in Advent Technology" Vol :12 Feb 2014.

[3]. Rampal sigh, Sawan Kumar, Shani Kumar "Ensuring Data Storage in cloud computing" IOSR Journal of Engineering Vol 2 Issue 12 Dec -12

[4]. G. Ateniese, R. Di Pietro, L.V. Mancini, and G. Tsudik. Scalable and efficient provable data possession. In *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks*, SecureComm '08, New York, NY, USA, 2008.

[5]. D. Abts and B. Felderman. A guided tour through data-centernetworking.*Queue*, 10(5):10:10–10:23, May 2012.

[6]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re- encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, 9:1–30.

[7]. "Security on cloud computing using Cryptography" vol 5 March 2015 Harneet kanar, Akash Desh mar.

[8]. R. Attebury, J. George, C. Judd, B. Marcum, and N. Montgomery. Google docs: a review. *Against the Grain*, 20(2):14–17,2008.

[9]. Aviram, S. Hu, B. Ford, and R. Gummadi. Determinating timing channels in compute clouds. In *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, CCSW '10, pages 103–108, New York, NY, USA, 2010.ACM.

[10]. "ID-Based Cryptography for Secure Cloud Data Storage "Nesrine Kaaniche, Aymen Boudguiga, Maryline Laurent. Springer 2015