ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

Accessing Secured Public Data Storage Using Secure Index in Cloud Computing Environment

M Rajasekar[1], Dr M Karthikeyan[2]

Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem, India[1]

Assistant Professor, PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem, India[2]

ABSTRACT: Number of company's different kind of data stored in cloud today. In last few years cloud providers provides the features of scalability, easy to use, fast access, flexibility and reduce the maintenance cost. Since biggest challenge at this stage are providing privacy and gives data security in public cloud servers. In this paper handled the efficient encryption technique for data owners and cloud providers using secret index key. In this paper discuss the two way encrypting technique similar to the hashing function. One for data owner and another one for cloud providers. The proposed scheme secured to the unauthorized modification detection and also unable to read encrypted data in cloud providers. Data access control only by data owner.

KEYWORDS : Privacy; Encrypiton; Data access control; Hash function; Secret index key.

I. INTRODUCTION

Cloud computing is a model for allowing convenient, on-demand access from anywhere, to a shared pool of computing services. These can include servers, storage, networking, applications and services. Cloud computing can be separated into three subsections such as cloud, data owner and users. Users and data owners can connect to the cloud environment via the internet. Cloud environment users uses the elasticity and multi-tenancy are two key features.

Service Models :

SAAS : Software as a service is also called a delivery Model. Here the software and data hosted over the cloud environment. Saas applications and data get from anywhere at any time via the different king of devices like mobile, tab and work station.

PAAS : Platform as a service access to a software development environment to allow them to create their own cloud applications. Paas applications are control over configuration settings for the application hosting environment. Example of paas : cloud foundry, Google App engine.

APPLICATION	IAAS	PAAS	SAAS
DATA	IAAS	PAAS	SAAS
RUN TIME	IAAS		SAAS
MIDDLEWARE	IAAS		SAAS
OPERATING SYSTEM	IAAS		SAAS
VIRTUALIZATION			SAAS
HARDWARE			SAAS
STORAGE			SAAS
INTERNET			SAAS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

IAAS : Infrastructure as a service is allows quickly and easily provision full computing resources, including processing, storage and networks. The user without having the management or control. Example of Iaas :SuseOpenstack cloud, IBM blue cloud.

Deployment Models:

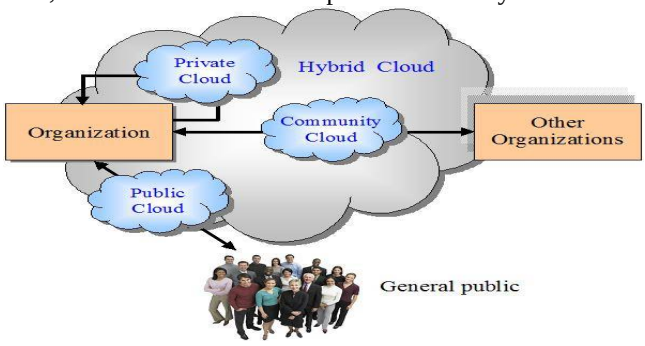
- Public model,
- Community Cloud,
- Private model,
- Hybrid model

Public model:

This infrastructure is available to the general model. Public cloud benefits are cost effective, reliability, high scalability, utility style costing, flexibility and location independence.Public cloud resources are access to everyone and anywhere.

Private model:

Private model is an get the most benefit in private organizations. Big enterprises usually used this model. This kind of service is not accessed by everyone, only access to under privileges. Private cloud model advantages are higher security and privacy, more control, coast efficiencies and improved reliability.



Cloud Service Delivery Model

Community cloud:

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, policy, security requirements, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community or some combination of them, and it may exist on premises or off premises.

Hybrid model:

Hybrid clouds are combination of private and public cloud in a same network. Hybrid model advantages are scalability, security, coast efficiencies and flexibility.

Characteristics :

Cloud computing have five essentials characteristics.

On-demand self-service:

This allows user to quickly and aromatically get access to the IT resources. They want without requiring in additional human interaction.

Broad network access:

This is ability to access a service from any standard device. This connects to the network including pc, laptops and tablets.

Resource pooling:

Compute, networking and storage are pooled are shared multiple customers.

Rapid elasticity:

This allows quickly scale the capabilities of your cloud match the level of user demand.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

Metering:

This control to the level of usage and cost of usage.

II. LITERATURE REVIEW

Searching encrypted data in a cloud is one of the biggest issues in the cloud environment. Efficient Cryptographic Technique for Securing and Accessing Outsourced Data [3]: Efficient encryption system that enables searching and moving encrypted data without violations of privacy. This system is working in an untrusted environment. The untrusted server cannot learn anything about the encrypted data and encrypted queries. This system is achieved through the use hashing technique, which enable the answering of queries in constant time regardless of the data size.
Practical techniques for searches on encrypted data [11]: The Authors song et al. have been first study of this problem. Song et al used a symmetric encryption method for word-by word encryption. Encryption of text and storage the resulting blocks of file. In this method clients are check the content sequential block-by-block search was conducted. Main disadvantages of this method searching on large data are not possible of this practical procedure.
Efficient Tree search in encrypted data [15]: The author Brinkman et al developed and algorithm for XML format in searching encrypted database.
Building secure indexes for searching efficiency on encrypted compressed data [[13]: The author Goh used a trapdoor generated by a secret key in his efficient secure searching technique over encrypted data and developed a secure indexing model. This method allows checking if a particular word is present in searched data in a single operation and provides semantic security. The trapdoor is the only way to find anything from the index but this method support single keyword search does not support this method to multiple keywords search.

Public-key encryption with keyword search [14]: Boneh et al devised a searchable public key encryption schema based on a sequential search on the server. The author developed two the two techniques, i)bilinear maps, ii) trapdoor permutations.

PKI based mechanism [15, 16]: PKI based encryption technique is an allows to the clients direct access to cloud data and remote access to the dynamic management of distributed resources and access.Trusted Cloud Computing Framework For Healthcare Sector [17]: The author Bamiah et al developed on fly encryption of data storage server, and used a multi-factor authentication schema for access control and security control mechanisms.

AlZain et al. [18] and Akshay et al. [19] conducted survey related to cloud security issues and addressed possible solutions for these issues.

III. PROBLEMSTATEMENT

A number of researchers devised secure index methods with keyword indexes saved on the cloud server. A number of methods have been developed to resolve data security and access control issues in cloud computing environment[5-10]. Searching encrypted data is not a simple work and also today it's not a possible task in cloud environment. The client may need to some data, usually download all data from cloud server to the local device then only decrypt it, and then search can be performed. Whenever the client need some data that time download the encrypted data and decrypt locally. In this encrypted method is not satisfies to the lower bandwidth users, low storage computer users and mobile users also not acceptable. This research is based on author's previous theoretical work [1, 3]. In this method wastageof time, effort and bandwidth.

IV. PROPOSED SYSTEM

The aim of this research paper is to develop an encryption mechanism using the secure index key to block-by-block. In this method users can possible to search encrypted data in public cloud environment.Organizations must encrypt the data preceding storage of their data on a public cloud server. The proposed data encryption schema is using two encryption keys: one for the data owner and the other for the cloud service provider. Two keys must be used to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

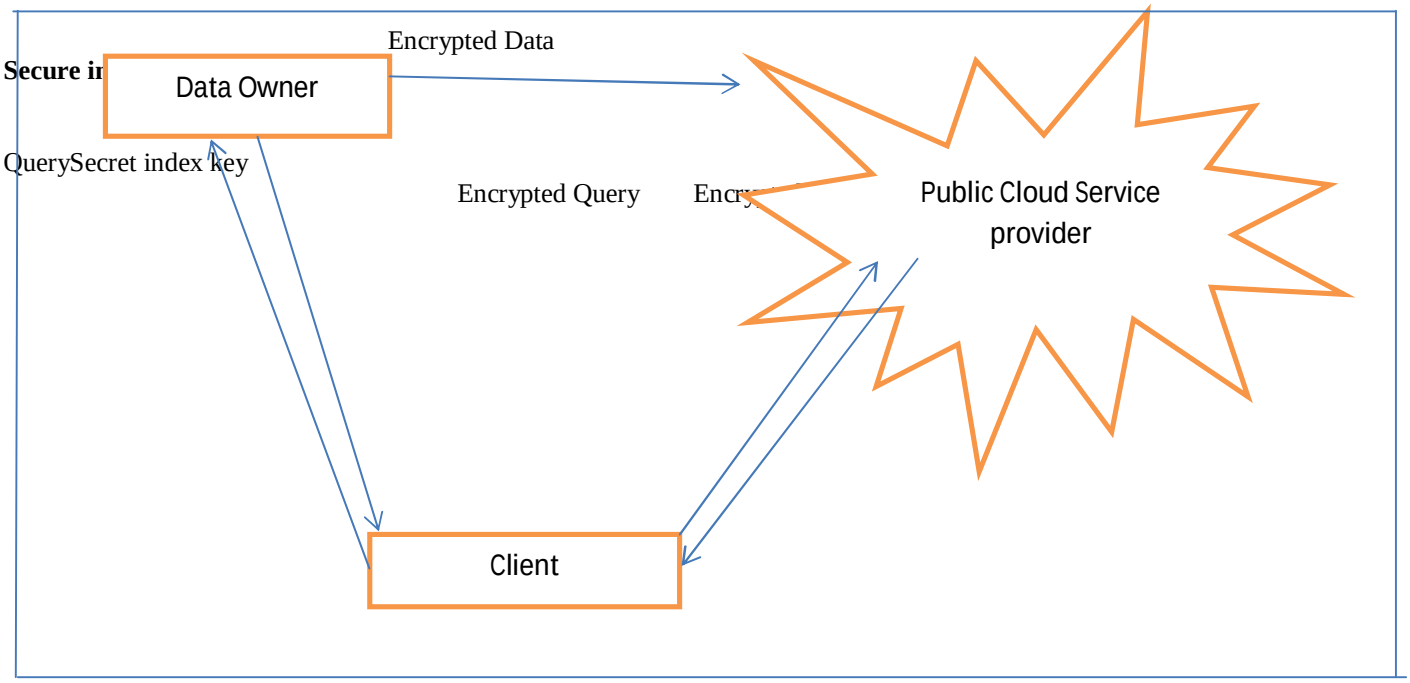
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

access the data. Only the owner can update and modify data. The service provider cannot view and modify the database content, thus guarantee read-and-write access privacy.



Architecture of a data outsourcing system

Data Owner :

Data owner can be outsourcing data onto a cloud server. Outsourcing data responsible for encrypting data at data owner module. The data are stored in public cloud server. Data owner only access to the encrypted data for loading and updating. Encryption algorithm for each identifier associated with each block of data and also generate to the encrypted index to encrypt each block of data.

Let's assume the data owner chooses two secret key T and Y. The secret key T is used to the one way hash function and also assume that outsourced data contain n identifiers for each blocks (ID1,B1;ID2,B2;…IDn,Bn). Y to generate the index key for each block of data.

Encrypted index:

Calculate Ki=HID(T,IDi), where HID(T,IDi) is collusion-free one way hash function, Ki is secret key for one way hash function. The hash function takes an input and output a short fixed length hash value.

$$nXi=HID(T,IDi) \oplus Y$$

Encrypted block:

Calculate Si= Ki⊕Bi where Si is encryption of HID(T,IDi)⊕ Bi,where ⊕is the XOR operation. The data owner responsibilities for encryption of data and data operations, it not depend on cloud service provider. Data owner need to perform various operations such as insert, modify, delete.

The insert operation such done that similar to the preparing encrypted data loading. To insert an new block of data Bi with takes identifier IDi,

$$nSi = Ki \oplus Bi$$

To remove the block of data Bi from outsourced data, the owner calculates the sub identifier Idi the sends the delete operation to the cloud service provider. The cloud service provider to find the index IDi, and then remove the encrypted block (Si).

Cloud Service Provider:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

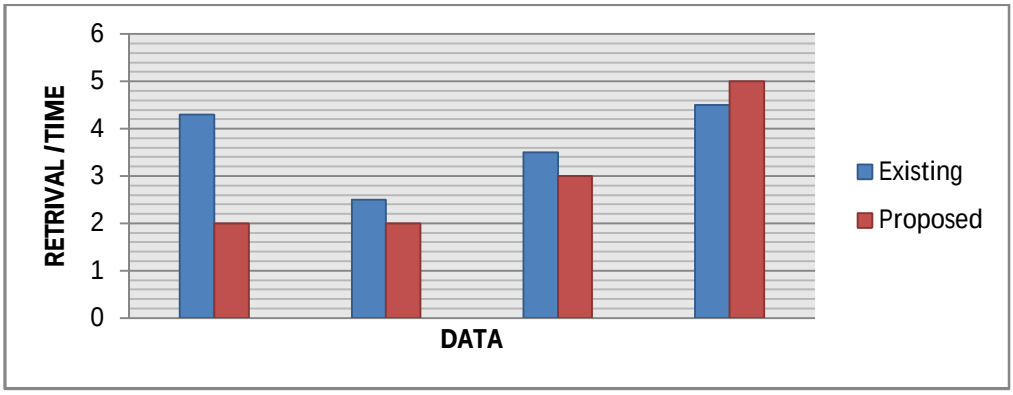
Data owners are encrypted data stored on the cloud servers that encrypted data are block-by-block. Cloud service providers also encrypt the encrypted data before store the cloud storage server. The service provider cannot derive any information from encrypted data and encrypted index.

Clients:

Trusted parties only to the access cloud data. Authentication of the client conducted by the data owner and then gets the secret user id and password via email or mobile phone. Only the legitimate clients are allowed to access the cloud. Client sends to the encrypted query to data owner for request. The data owners aresending to the encrypted index for client needed data. Clients are downloading the needed data only in local system. There is no need to download all the encrypted data. The search is conducted and gets the data from the cloud.

V. RESULT AND DISSCUSSION

Two way encryption methodsare very secure to the data privacy in unauthorized users. Since solutions are run by the cloud provider, cloud providers have an obligation to both their clients and Data owners. The cloud atmosphere, the cloud user must have enough data and visibility into the cloud provider's system to be ready to provide reports to regulators and to their own clients. Logging is a very important role in the proper operation of ansecure information processing system. In this paper, we proposed a complete system to securely outsource log records to a cloud provider. Index key encryption mechanism as gives the high privacy in compare with existing system.In proposed a comprehensive scheme that addresses security and integrity issues not just during the log generation phase, but also during other stages in the information encryption management process, including log collection, accessing the information, transmission, storage, deletion and retrieval. One of the unique challenges is the problem of data privacy in cloud storage arises. Data Owners provided anonymous upload, retrieve and delete protocols on log records in the cloud network. Current implementation of the logging client is loosely coupled with the operating system based logging.



V. CONCLUSION

Security of the outsourced data in public cloud storage has been examined in this paper. Two way encryption mechanismsallows secure and efficient access to cloud data. The data owner takes all control of data, and no actions of the cloud service provider. In this paper each block of data can be encrypted using encrypted index. Main advantage of the proposed system reduces communication overhead and computations on both client and service providers. The main focus of this paper security of public cloud data, do not gives the permission to access the untrusted clients and benefit from a service provider overhead.

REFERENCES

[1] Al-Sakran, Hasan Omar,Accessing Secured Data In Cloud Computing EnvironmentInternational Journal Of Network Security & Its Applications (Ijnsa) Vol.7, No.1, January 2015

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

[2] Dakhane, D.M. & A.A. Arokar, (2012) "Data Secuity in Cloud Computing for Biometric Application Application," International Journal of Sci Research, Vol. 3, No. 6, pp. 1-4.
[3] Al-Sakran, Hasan Omar, Bin Muhaya, Fahad& Irina Serguievskaia, "Efficient CryptographicTechnique for Securing and Accessing Outsourced Data", International Journal of Computer Science and Information Security, Vol. 9, No. 8, August 2011.
[4] Wang, W., Li, Z., Owens, R. & B. Bhargava, (2009) "Secure and Efficient Access to Outsourced Data", in Proc. of ACM Cloud Computing Security Workshop, pp. 55-65.
[5] di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S. & P. Samarati, (2007) "A data outsourcing architecture combining cryptography and access control", in Proc. of the ACM workshop on Computer Security Architecture, pp. 63-69.
[6] S di Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S. & P. Samarati, (2007) "Over-Encryption: Management of Access Control Evolution on Outsourced Data", in Proc. of the International Conference on Very Large Databases, pp. 123-134.
[7] Yin, X. Z.; Liu, H. & Jae Lee, (2014) "An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI", IEEE 16th International Conference on Advanced Communication Technology (ICACT) , pp. 523 – 527. International Journal of Network Security & Its Applications (IJNSA) Vol.1, No.1, January 2015 28
[8] Yang, Ching-Nung&Jia-Bin Lai, (2013) "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", International Symposium on Biometrics and Security Technologies (ISBAST), pp 259 – 266.
[9] Ullah, S. & Z. Xuefeng, (2014) "TCLOUD: A Trusted Storage Architecture for Cloud Computing", International Journal of Advanced Science and Technology Vol.63, pp.65-72
[10] Dang Tran Khanh, (2009) "Security issues in outsourced xml databases". In Open and Novel Issues in XML Database Applications: Future Directions and Advanced Technologies. IGI Global,.
[11] Song, D.; Wagner, D. & A. Perrig, (2000) "Practical Techniques for Searches on Encrypted Data", in Proc. of the 2000 IEEE Symposium on Security and Privacy (S&P 2000).
[12] Brinkman, R.; Feng, L.; Doumen, J.M., Hartel, P.H. & W. Jonker, (2004) "Efficient Tree Search in Encrypted Data", 2nd International Workshop on R. Security in Information Systems, April 2004.
[13] E. Goh, (2003) "Building Secure Indexes for Searching Efficiently on Encrypted Compressed Data", http://eprint.iacr.org/2003/216/
[14] Boneh, D.; Crescenzo, G. D.; Ostrovsky, R. & G. Persiano, (2004) "Public-key encryptionwith keyword search", In: C. Cachin, editor, Proceedings of Eurocrypt 2004, LNCS, Springer-Verlag, May 2004.
[15] Dai, J. & Q. Zhou, (2010) "A PKI - based Mechanism for Secure and Efficient Access to Outsourced Data", 2010 International Conference on Networking and Digital Society.
[16] Yin, XiaoChun; Lui, ZengGuang&Hoon Jae Lee, (2014) "An Efficient and Secured Data Storage Scheme in Cloud Computing Using ECC-based PKI", IEEE 16th International Conference on Advanced Communication Technology (ICACT), pp 523 – 527.
[17] Bamiah, MervatAdib; Brohi, Sarfraz Nawaz; Chuprat, Suriayati& 2Jamalul-lail AbManan,(2014) "Trusted Cloud Computing Framework For Healthcare Sector". Journal of Computer Science Vol. 10, No 2, pp 240-250.
[18] AlZain, M.A.; Soh, B. & E. Pardede, (2013) "A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", Journal of Software, Vol. 8, No. 5, May 2013
[19] Kapse, Akshay D. &Piyush K. Ingole, (2014) "Secure and Efficient Search Technique in Cloud Computing", Fourth International Conference on Communication Systems and Network Technologies, pp 419 – 429.