

Accessing Data from Cloud using Cryptography

Preeti Jain¹, Dr. BarjeshKochar²
Research Scholar, JNU, Jaipur¹
Professor, IT Dept., JIMS, Rohini, New Delhi²

Abstract: The aura of cloud computing has been touching hearts of many companies and organization day by day. Being flexible, scalable and easy to use plug in play services, customers are getting addicted to various cloud services. The paper presents cryptography system that uses encryption technique for assessing data securely from public cloud environment. Encryption involves transfer of data into some coded cipher form that is not understandable by local users located on public clouds. Only data owner can provide access to different users by decrypting it with its unique password on key.

Keywords: Cryptography, Encryption, Decryption, public cloud and Hash function

1. INTRODUCTION

With tremendous increase in latest technology trends, the consumption of resources has been increase to great height. Users are acquiring resources provided by cloud providers in order to perform task faster and increased efficiency rate. In addition to this, cloud deployment models also exist that has some features. If data center is owned and managed by some community or customer and users can

access data any time without taking permission, then it is called private cloud. If data center is accessed and managed by cloud services providers like Google, Amazon and users are willing to use their services by asking for permission then it is called as public cloud. Hybrid cloud is combination of either private or public cloud. Ensuring data confidentiality and authentication are one of major concerns for public cloud environment. Customers always suffer from fear that their data may be accessed by intruders or attackers. The solution to this concern is described in following paper that employs use of cryptographic process (encryption and decryption). In this process, data owner has its key that updates data (encryption) and for accessing that data, users are required to enter decryption key. The remaining paper is organized as follows. Section 2 presents previous studies in context of cloud computing. Section 3 deals with proposed cryptographic system. Section 4 presents list of related works that have been done in

order to prove our system better. Section 5 concludes the given paper.

2. LITERATURE SURVEY

Various studies have been lead by researchers in context of security issue and schemes for achieving confidentiality. Song et.al [1] revised encryption method for securing data. They analyzed text by text and encrypt them using key at client site as well as server site. It is very time consuming process. Brinkman et.al [2] suggested idea of creating indexing on blocks of file and developed algorithm for searching databases. Goh et.al [3] proposed secure indexing model by using encryption technique without involving use hash function. Keu yang et.al [4] proposed data access control mechanism for storing data secured key. Alizarin et.al [5] have lead various studies in context of security issue of cloud computing. Ruj et.al [6] used concept of decentralization in order to access data from random users. But it may lead to risk of intruders attackers. Although cloud is best platform for storage of resources but without its security it is of no use. Cloud computing services must be improved in legal protection also [7].

3. Comparison of existing works

Study	Features	Proposed System
Ruj et.al [6]	Decentralized process to access data. No client – service provider awareness	Centralized system with interoperability between client and service providers.
Goikar et.al [18]	Uses GPS receiver to find location of data and decrypt it. If location not found, then data cannot be accessed.	Uses hash function to search for data sequentially and maps values to different locations. If data is not found at given location, then it moves to next location rather than stopping process.
Goh et.al [3]	Used trapdoor to search for data but not suitable for multiple keywords search.	Handles multiple keyword searches.
Boneh et.al	Performs sequential	Performs

[20]	search of data by using bi-linear maps. Bi-linear maps has disadvantage that they may point to multiple locations with same time periods.	sequential search using one-way collision free hash function that points to multiple locations at different time periods.
------	---	---

- The existing work employs use of bi-linear maps to point data values to different locations but at same time. It leads to collision because it may happen that second location is already having data at same time.
- The generation of metadata has not properly utilized as it lacks encrypted data index file.

4. Flaws in the existing work

The existing work in context of accessing data from cloud using cryptography process has been mentioned in [3, 6, 18, and 20]. The flaws in their works are as follows:

- There is no centralized system designed for interaction between client and server and to prevent data loss.
- The process gets ceased if data is not found or located at given memory locations. It ceased due to lack of one way hash function. It would be better to employ use of hash function for mapping data values at different memory locations.

5. PROPOSED CRYPTOGRAPHIC SYSTEM

The system deals with owner/manager, client and cloud service provider (Google/yahoo). Client acts as interface between owner and service provider. The proposed framework is required to keep data protected from third parties and it should reach at client site. Then client can forward that data to cloud provider in order to get original data. The detail layout is given below:-

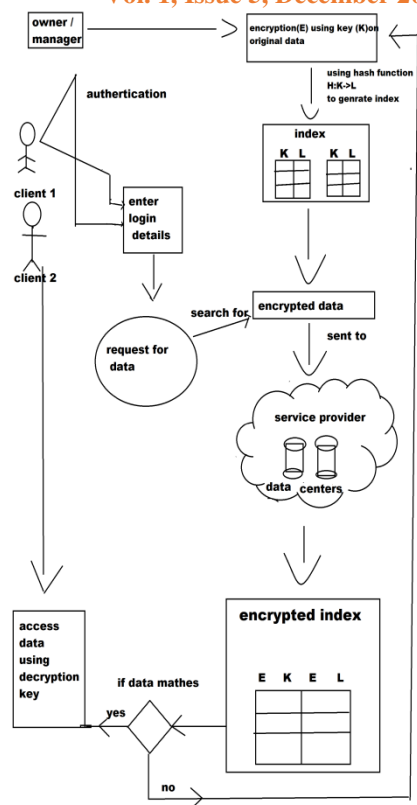


Fig 1: Layout of proposed work

6. Working

The data owner has right to send, manage and access data any time. Firstly, data is being put in query to be sent to service provider. It has to undergone through process of encryption before data is being sent to provider. Data owner has it's secrete key (K) that is used as identifier to generate cipher text (codedtext) using process of encryption (E). Indexing is being done to access data in less time. It can be done using hash function. Hash function maps value to different locations a service provider.

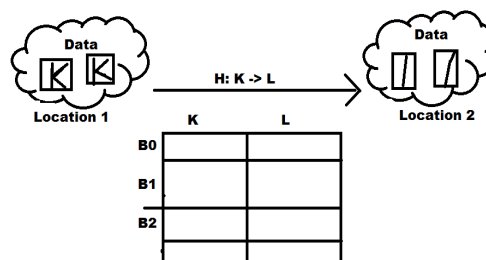


Fig 2: Process of Indexing

Blocks of data stored as indexes on given locations now, encrypted data values are stored in index field. This encrypted data is being sent to cloud service provider stores data to various remote locations hosted by different data centers. As soon as data reaches provider, it generates index of encrypted data at its site. This encrypted data is being searched by different clients that are requesting for data. Then client uses decryption key provided by data owner and access that matched encrypted data.

7. How proposed system overcomes existing flaws or advantages of proposed system

- The system tests malicious data sent from untrusted sites by involving the process of encryption.
- The process of encryption generates cipher text that is not understood by third parties except

data owner. Only data owner can access that data because it has its own secret key (K).

- The system is centralized rather than decentralized. It means client and service providers maintain interoperability to access data securely. If system is made decentralized, then it might be possible that service providers keep waiting for encrypted data which is requested by client before.
- The proposed system is able to handle multiple search keywords. If user enters two queries, they are being put into queue for undergoing process of encryption. Rather than generating hash index for one query, it produces two hash indices for two queries. If both hash functions map to same locations in memory, then data at that location is recorded with different time period. Data with earliest time is being accessed by client firstly and its memory location gets filled by other key value.

8. Conclusion and future scope

The paper presents a technique to achieve secured data from public cloud environment. Security is major concern that needs to be improved by cloud standards. Various studies are going on regarding this. A cryptographic system has been proposed in following paper. It makes use of encryption when data is sent by owner to service provider at service provider site. It uses one way hash function that helps in creating index of blocks of data at various remote location hosted by data centers for accessing this data, cloud service provider again maintains index of encrypted data at that time client request for data and if searching data get matches with encrypted data, then client can access data using its decryption key.

The proposed system can be made interoperable with semantic web security standards in which data can be accessed using lightweight ontology's in machine understandable format.

9. REFERENCES

- [1]. 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)
- [2]. 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.
- [3]. E. Goh, (2003) "Building Secure Indexes for Searching Efficiently on Encrypted Compressed Data", <http://eprint.iacr.org/2003/216/>
- [4]. Yang ,Kan; Jia, Xiaohua; Ren, Kui& Bo Zhang, (2013) "DAC-MACS: Effective data access control for multi-authority cloud storage systems", INFOCOM, 2013 Proceedings IEEE , pp 2895 – 2903
- [5]. 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
- [6]. Ruj, S.; Stojmenovic, M. & A. Nayak, (2014) "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds), IEEE Transactions on Parallel and Distributed Systems, pp 384 – 394.
- [7]. Michael Gregg, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Global Knowledge, 2010
- [8]. "Security and high availability in cloud computing environments" , IBM Global Technology Services Technical White Paper ,IBM ,June 2011
- [9]. V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.
- [10]. Meiko Jensen, JörgSchwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing
- [11]. 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
- [12]. 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
- [13]. 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

[14]. Bamiah, MervatAdib; Brohi, Sarfraz Nawaz; Chuprat, Suriayati&Jamalul-lailAbManan, (2014) “Trusted Cloud Computing Framework For Healthcare Sector”. Journal of Computer Science Vol. 10, No 2, pp 240-250

[15]. Meer Sohei 1 Abolghasemi, Mahdi sefidab, Reza EbrahimiAtani, “Using Location Based Encryption to Improve the Security of Data Access in Cloud Computing”, international conference on advances in computing 2013

[16]. GurudattKulkarniet al, “Cloud Security Challenges”, 7th International Conference on telecommunication systems, Services and Applications(TSSA),IEEE,2012

[17]. RajnishChoubey et al., “A Survey on Cloud Computing Security, Challenges,

Threats”, International Journal on computer Science and Engineering(IJCSE)2011

[18]. Goikaret.al , “Improve Security of data access in cloud computing using location”, International Journal of Computer science and mobile computing (IJCSMC), Feb 2015, pp 331-340.

[19]. Y, Amanatullah, Ipung H.P., Juliandri A, and Lim C. "Toward cloud computing reference architecture: Cloud service management perspective.". Jakarta: 2013, pp. 1-4, 13-14 Jun. 2013

[20]. Boneh, D.; Crescenzo, G. D.; Ostrovsky, R. & G. Persiano, (2004) “Public-key encryption with keyword search”, In: C. Cachin, editor, Proceedings of Eurocrypt 2004, LNCS, Springer-Verlag, May 2004