Privacy Protection Based Hierarchical and Shared Access Control Scheme in Cloud-Based Services

Poornima G. Pawar[1] , Vikas Thombre [2]

[1]*Computer Engineering Department, SKNSITS, Lonavala, India*

[2]*Professor, Computer Engineering Department, SKNSITS, Lonavala, India*

Abstract

Cloud computing offers flexible computation and resources for storage purpose, but here user poses challenges on variability of computations and data privacy. Because of data privacy reason some data owner away from cloud facility. Existing system is only encrypted and decrypts data on attribute base. In proposed system a hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario. Our system model consists of four types of parties: data owners, users, a root authority and a number of domain authorities. The analysis results show the proposed scheme is efficient, scalable, and fine-grained in dealing with access control for outsourced data in cloud computing.

Keywords: *Domain, Authority, fine-gained, secret Share.*

1. Introduction

Cloud computing is the delivery of computing and storage space as a service to a distributed community of end users [1]. The schema/model of Cloud computing is, all the servers, networks, applications and other elements related to data centers are made available to end users. Cloud computing is growing now-a-days in the interest of technical and business organizations but this can also be beneficial for solving social issues. Cloud computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application [10].

The current network-centric world has given rise to several security concerns regarding access control management, which ensures that only authorized users are given access to certain resources or tasks. Based on their respective roles and responsibilities, users are typically organized into hierarchies composed of several disjoint classes[14]. We have characterized a hierarchy by the fact that some users may have more access rights than others, according to a top-down inclusion paradigm following specific hierarchical dependencies[14]. It provide security and performance analysis of our proposed scheme by Secret Shares Algorithm and data encryption method The user only get the secret key by providing the certain pieces of secret shares to download the decrypted data.

In existing system enhances a general approach to protect the data is encryption methodology, they are keyword based encryption system and it supports for plain text data [3][17]. Fully homomorphism encryption is used to solve the problem of the data user. Searchable encryption schemes are very efficient, its functionality and security is well and also allows users to search in the cipher text in cloud storage.

2. Literature Review

In Ensuring security and privacy preservation for cloud data services researched by J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya ; With the rapid development of cloud computing, more and more enterprises/individuals are starting to outsource local data to the cloud servers. However, under open networks and not fully trusted cloud environments, they face enormous security and privacy risks (e.g., data leakage or disclosure, data corruption or loss, and user privacy breach) when outsourcing their data to a public cloud or using their outsourced data. Recently, several studies were conducted to address these risks, and a series of solutions were proposed to enable data and

privacy protection in untrusted cloud environments. To fully understand the advances and discover the research trends of this area, this survey summarizes and analyses the state-of-the-art protection technologies. The first present security threats and requirements of an outsourcing data service to a cloud, and follow that with a high-level overview of the corresponding security technologies. We then dwell on existing protection solutions to achieve secure, dependable, and privacy-assured cloud data services including data search, data computation, data sharing, data storage, and data access. Finally, we propose open challenges and potential research directions in each category of solutions.

A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data .Z. Xia, X. Wang, X. Sun, Q. Wang published The major aim of this paper is to solve the problem of multi - keyword ranked search over encrypted cloud data (MRSE) at the time of protecting exact method wise privacy in the cloud computing concept[2] . Data holder s are encouraged to outsource their difficult data management systems from local sites to the business public cloud for large flexibility and financial savings. However for protecting data privacy, sensitive data have to be encrypted before outsourcing, which performs traditional data utilization based on plaintext keyword search. A s a result , allowing an encrypted cloud data search service is of supreme significance . In vie w of the large number of data users and documents in the cloud, it is essential to permit several keywords in the search demand and return documents in the order of their appropriate to these keywords. Similar mechanism on searchable encryption makes center on single keyword search or Boolean keyword search, and rarely sort the search results[5]. In the middle of various multi - keyword semantics, deciding the well - organized similarity measure of "coordinate matching," it means that as many matches as possible, to capture the appropriate data documents to the search query.

In Privacy-preserving traffic padding in web-based applications research by W. M. Liu, L. Wang, P. Cheng, K. Ren, S. Zhu, M. Debbabi said Web-based applications are gaining popularity as they require less client-side resources, and are easier to deliver and maintain. On the other hand, web applications also pose new security and privacy challenges [3]. In particular, recent research revealed that many high profile web applications might cause sensitive user inputs to be leaked from encrypted traffic due to side-channel attacks exploiting unique patterns in packet sizes and timing. Moreover, existing solutions, such as random padding and packet-size rounding, were shown to incur prohibitive overhead while still failing to guarantee sufficient privacy protection. In this paper, first observe an interesting similarity between this privacy-preserving traffic padding (PPTP) issue and another well studied problem, privacy-preserving data publishing (PPDP). Based on such a similarity, we present a formal PPTP model encompassing the privacy requirements, padding costs, and padding methods. We then formulate PPTP problems under different application scenarios, analyse their complexity, and design efficient heuristic algorithms. Finally, we confirm the effectiveness and efficiency of our algorithms by comparing them to existing solutions through experiments using real-world web applications.

Enabling privacy-assured similarity retrieval over millions of encrypted records X. Yuan, H. Cui, X. Wang, C. Wang published Searchable symmetric encryption (SSE) has been studied extensively for its full potential in enabling exact - match queries on encrypted records. Yet, situations for similarity queries remain to be fully explored. In this paper, design privacy - assured similarity search schemes over millions of encrypted high - dimensional records. Our design employs locality - sensitive hashing (LSH) and SSE, where the LSH hash values of records are treated as keywords fed into the framework of SSE. As direct combination of the two does not facilitate a scalable solution for large datasets, we then leverage a set of advanced hash - based algorithms including multiple - choice hashing, open addressing, and cuckoo hashing, and craft a high performance encrypted index from the ground up. It is not only space efficient, but supports secure and sufficiently accurate similarity search with constant time. Our designs are proved to be secure against adaptive adversaries. The experiment on 10 million encrypted records demonstrates that our designs function in a practical manner.

In Enabling secure and efficient ranked keyword search over outsourced cloud data

C. Wang, N. Cao, K. Ren, W. Lou ; the statistical measure approach, i.e. relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. Recent technological developments in cloud computing and the ensuing commercial appeal have encouraged companies and individuals to outsource their storage and computations to powerful cloud servers. We focus in particular on the scenario where a data owner wishes to outsource its public database to a cloud server; enable anyone to submit multi-keyword search queries to the outsourced Database and ensure that anyone can verify the correctness of the server's responses.

In Attribute based access control with constant size cipher text in cloud computing
Wei Teng, Geng Yang, Yang Xiang, Senior Ting Zhang and Dongyang Wang;
With the popularity of cloud computing, there have been increasing concerns about its security and privacy. Since the cloud computing environment is distributed and untrusted, data owners have to encrypt outsourced data to enforce confidentiality. Therefore, how to achieve practicable access control of encrypted data in an untrusted environment is an urgent issue that needs to be solved. Attribute-Based Encryption ABE is a promising scheme suitable for access control in cloud storage systems. This paper proposes a hierarchical attribute-based access control scheme with constant-size ciphertext. The scheme is efficient because the length of ciphertext and the number of bilinear pairing evaluations to a constant are fixed. Its computation cost in encryption and decryption algorithms is low. Moreover, the hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario.

3. Motivation

A well-known principle in the analog world is the term reduced trust, meaning that in order to keep a secret, the less knowledge or power each entity is the better. This is the basic philosophy, and we shall study how it is implemented in the digital world as well.

4. Proposed Approach

In proposed an access control system, which is privilege separation based on privacy protection.

A number of hierarchical authorisation structures are also presented, which can be used in organizations or companies to meet the requirement of authorization grant right decentralization.

The domain authorities will distribute the security parameters to users or sub-domain authorities.

In proposed an efficient construction for those schemes, denoted as Secret Shares Algorithm in Encryption Based Construction, which assigns to each class a single private information, whereas, the public information depends on the number of classes, as well as on the number of edges in the hierarchy.

The security of the proposed construction relies on the ones of the underlying encryption and secret sharing schemes using Shamir Secret Sharing Algorithm.

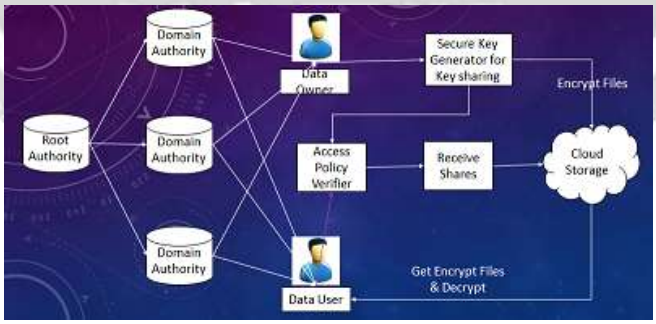

Fig.1: System Architecture

4.1 Algorithm:

Input:

K = Domain Root

DA = No. of Domain Authority No. authorized by K

Do= No. of Domain owners authorized by [A]

DU= No. of domain user authorized by $[Do]_n$

Processing:

Step1: Create Root Domain.

Step2: Add Domain Authority

Da=1 to N

Step3: Add domain Owner and Domain User.

3.1: Create Multiple Domain Owner under DA

3.1.1: Encrypt Data File

3.1.2: Secret shares key

For(int i =1; i < maxprime; i++)

3..1.3: upload file in cloud

Share[x-1]=[x,accum]

accum= bigInteger value

3.2: Create Multiple Domain User under DU

3.2.1: Send data access request.

3.2.2: Secrete share verification.

3.2.3: Download data.

3.3: verify Access Policy [If i > && i < s.length-1]

(Retrieve file size.)

5. Results

Figure 5.1 shows Existing system ;the encryption algorithm is depend on private key .size of the attribute depends linearly on the number of attribute in other scheme. The length of secret key grow quadratically with the number of attributes.

Figure 5.2 shows Proposed work which having better than existing system.In existing length of share key depends on the number of attributes; means its requied total time to encryption depend on size of the file.we observed that we have taken different file types like .xls,.pdf,.txt,.doc etc

Which have taken to upload file as average 1 to 2 nanosecond.secret key having fix size which was genereated up to 2ns. Encryption file is depend on total file size which we want to encrypt data.In result, Sharing key time and Downloading time both are same.image file required less time thand text and pdf file.

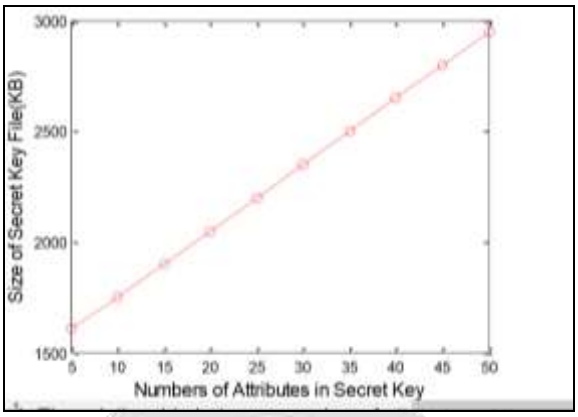

Figure 5.1: Existing System

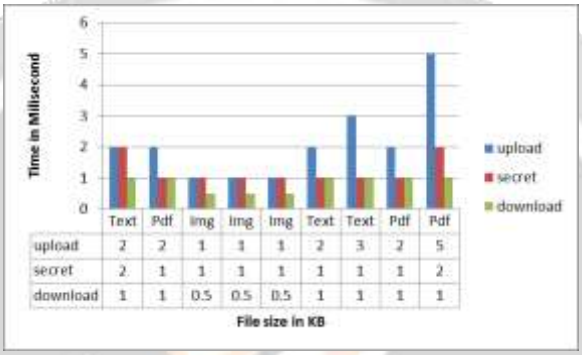

Fig. 5.2: Proposed System

6. CONCLUSION AND FUTURE WORK

Secure sharing of data plays an important role in cloud computing, it can realize data confidentiality in the untrusted environment of server-end, fine-grained access control and large-scale dynamic authorization which are the difficult problems to solve the traditional access control. This paper proposes a structure of hierarchical authority based on cloud computing which reduces the burden and disperses the risk of the single authority. In addition, we have implemented Shamir Secret Sharing Algorithm for high level security, this shows our scheme has good adaptability and scalability in cloud computing. Our scheme has lower computational and communication overhead, which has a promising future in secure authentication in cloud big data. In further research, we intend to focus on making the Secret Sharing algorithm simpler and more efficient along with making it even more suitable for access control in a cloud environment.

ACKNOWLEDGMENT

It gives me great pleasure to deliver sincere thanks to my project guide Prof. V.D.Thombre for his valuable guidance, constant encouragement and support. I appeal thanks to all the authors of the referenced papers as they help me and motivate me to work on this emerged area. Last but not least, I would like to deliver thanks to my family members, my colleague, and the people who directly or indirectly support me in this project work.

REFERENCES

1. Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing Wei Teng, Geng Yang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Ting Zhang and Dongyang DOI 10.1109/TCC.2015.2440247,
2. S. Brin and L. Page, "The anatomy of a large-scale hyper textual web search engine," Computer Networks and ISDN Systems, vol. 30, no. 17, 1998
3. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SP 2000. Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55
4. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.
5. . Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506–522.
6. DY.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 442–455
7. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Kon-winski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010. Security. ACM, 2006, pp. 79–88.
8. J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications. Springer, 2008, pp. 1249–1259
9. W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure knn computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of Data. ACM, 2009, pp. 139–152.
10. S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+r: Top-k retrieval from a confidential index," in Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology. ACM, 2009, pp. 439–449
11. B. Yao, F. Li, and X. Xiao, "Secure nearest neighbour revisited," in Data Engineering (ICDE), 2013 IEEE 29th International Conference on, 2013, pp. 733–744
12. Data management with attribute based encryption method for sensitive users in cloud computing. Vidyasagar Tella,L.V Ramesh.IJETR ISSN:2321-0869,vol-2,issue-9,September 2014
13. A Literature Survey on key aggregation system for secure sharing of cloud data. Arun Kumar S., S. Dhansekar IJARECE ,vlo-3, issue-(12 ,December 2014)
14. A Literature Survey on key aggregation system for secure sharing of cloud data. Arun Kumar S., S. Dhansekar IJARECE ,vlo-3, issue-(12 ,December 2014)
15. An Efficient Presentation of Attribute Based Encryption Design in cloud data. ISSN:2277 128X, vol-5,issue-(2 Feb 2015)
16. An Efficient Presentation of Attribute Based Encryption Design in cloud data. ISSN:2277 128X, vol-5,issue-(2 Feb 2015)
17. Attribute based encryption Optimal for cloud computing(Mate Harvath) jan-5-2015
18. Attribute based access control (Prof. N.B. Kadu ,Gholap Nilesh, Saraf Shashir, Garodi Pravin ,Bora Anand. IJARIIE-ISSN(0)-2395-4396vol-2,issue-2 2016

BIOGRAPHY

Poornima G. Pawar.I have completed Bachelors in Computer science & Engineering (BE-CSE) from A.G.P.I.T College, Solapur University and currently pursuing ME in computers from SKNSITS, Lonavala. My research interests are Cloud computing , Database technologies, Software Project Management, Software Testing and Software Engineering.

Vikas Thombre, I have completed Bachelors in Computer Engineering (BE) from Government College Of Engineering, Aurangabad and masters (MTECH) in computer engg., from Dr. Babasaheb Ambedkar Technological University, Lonere. Currently, I am working as an assistant professor and HOD at SKNSITS, Lonavala with total experience of 11 years. My research interests are Data mining and information retrieval, Software Architecture and Software Engineering.