Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Comparative Analysis of Two Fine Grained Data Access Control Techniques in Cloud Computing

Mandeep Kaur
MTECH (CSE), Punjab Technical University
Punjab, India

Abstract— It is the model for convenient on-demand network access , with minimum management efforts for easy and fast network access to resources that are ready to use. Popularity of cloud computing is increasing day by day in distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. DM cloud is the process of extracting structured information from unstructured or semi structured web data sources. is the extraction of hidden predictive information from large databases. It helps the companies to focus on the most important in their data warehouses. It predicts future trends and behavior , allowing business to make proactive , knowledge- driven decisions .The KP-TSABE is able to solve some important security problems by supporting user-defined authorization period and by providing fine-grained access control during the period.

Keywords— Cloud computing, Data mining in Cloud, a KP-TSABE scheme, Advanced KP-ABE

I. INTRODUCTION

Cloud computing is the model for convenient on-demand network access, with minimum management efforts for easy and fast network access to resources that are ready to use. It is an upcoming paradigm that offers tremendous advantages in economic aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. Popularity of cloud computing is increasing day by day in distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Their main concerns are the confidentiality, integrity, security and methods of mining the data from the cloud. Cloud computing entrusts services with a user's data, software and computation over a network. Google Apps is one of the best examples of cloud computing where users can access software tools hosted on Google's data centres by using any connected device with a web browser or a mobile application.

Data mining in Cloud

DM cloud is the process of extracting structured information from unstructured or semi structured web data sources. Cloud providers use data mining to provide clients a better service. The data mining tasks you can perform with DM Cloud are the same Table Analysis Tools found in the traditional Excel Data Mining add-in. The data mining in Cloud Computing allows organizations to centralize the management of software and data storage, with assurance of efficient, reliable and secure services for their users. Here we explore the how the data mining tools like SAS, PAS and IaaS are used in cloud computing to extract the information. A cloud provider for a data mining and natural language processing system. Leading cloud computing providers Amazon Web Services, Windows Azure, Open Stack. People use this feature to build information listing, get information about different topics by searching in forums etc. Companies use this service to see what kind of information is floating in the World Wide Web for their products or services and take actions based on the data presented. Cloud computing allows the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage.

II. LITERATURE SURVEY

In the article [1] **"A secure data self-destructing scheme in cloud computing"** in Jan 2014 Jinbo Xiong, has proposed a KP-TSABE scheme, which is a novel secure self-destructing scheme for data sharing in cloud computing.It first introduce the notion of KP-TSABE, formalize the model of KP-TSABE and give the security model of it. Then, gives a specific construction method about the scheme. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. The KP-TSABE is able to solve some important security problems by supporting userdefined authorization period and by providing fine-grained access control during the period. The sensitive data will be securely self-destructed after a user-specified expiration time.

In the article [2] "**Secure Data Mining in Cloud using Homomorphic Encryption"** Deepti Mittal had proposed a method to solve the privacy issues of the cloud. It assumes that the user data is distributed on two hosts and performs a combined k-means clustering using the Pallier Homomorphic ncryption system for security purpose so as to prevent any interpretation of intermediate results by an attacker. The proposed approach can further be extended by adding a digital

signature or hashing technique to authenticate the third party so as to prevent an adversary from posing as the third party to host's. Also it can be generalized or extended to more number of hosts if required.

In the article [3] **"On Modeling Confidentiality Archetype and Data Mining in Cloud Computing** "in March 2013 "Alawode A. olaide" has proposed the concept of data mining in the cloud. This paper discus effort directed to which degree this skepticism is justified, by proposing to model Cloud Computing Confidentiality Archetype and Data Mining 3CADM. The 3CADM is a step-by-step framework that creates mapping from data sensitivity onto the most suitable cloud computing architecture and process very large datasets over commodity clusters with the use of right programming model.

In the article [4] **"An Approach to protect the privacy of the cloud data from data mining based attacks"** in April 2013 "Himeldev, Tanmoysen" has proposed the concept of privacy of the cloud data from data mining and attacks on the cloud data. We first identify the data mining based privacy risks on cloud data and propose a distributed architecture to eliminate the risks. The key idea of our approach is to categorize user data, split data into chunks and provide these chunks to the proper cloud providers. In a nutshell our approach consists of categorization, fragmentation and distribution of data.

In the article [5] **"Information Retrieval through Multi -Agent System with Data Mining in Cloud Computing"** in February 2012 "Vishal Jain and Mahesh Kumar" has proposed the concept of retrieving the useful information through Multi-Agent system. The paper will undertake a review of the existing literature available on this arena and develop an empirical model showing real time data flow through MAS with data mining after retrieval of meaningful information from data warehouse present in a cloud computing environment. In the end, paper will provide recommendations for the organizations for effective implementation and use.

In the article [6] **"Data mining in the cloud computing"** in April 2012 "Bhagyashree Ambulkar and Vaishali Borkar" has proposed the concept of mining of the data from the cloud. This paper deals with the study of how data mining is used in cloud computing. Data Mining is a process of extracting potentially useful information from raw data. We have recently seen an increase in data mining techniques targeted to such applications as fraud detection, identifying criminal suspects, and prediction of potential terrorists. By and large, data mining systems that have been developed to data for clusters, distributed clusters and grids have assumed that the processors are the scarce resource, and hence shared. When processors become available, the data is moved to the processors.

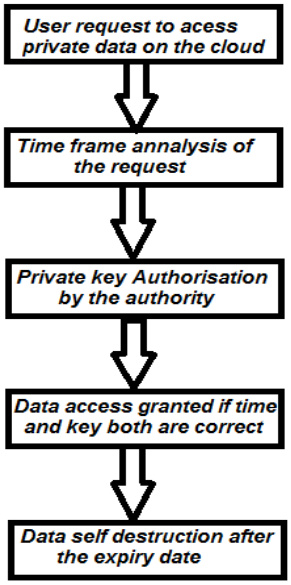
In the article [7] **"Mitigating Data Mining Attack in Cloud"** in April 2014 "A. Raja Rajeswari and R.Sakkaravarthi" has proposed the concept of data mining based privacy attacks in the cloud. As an alternative of maintaining personal data on the own hard drive or updating important applications for user needs, user can use a service over the network, to a different location, to store user information and / or use its applications. This also provides flexibility so it is very useful in a new generation of services and products. One of the main security problems in cloud is data mining based privacy attacks that involve analyzing data over a long period to extract valuable information.

III. COMPARATIVE ANALYSIS

System Model of KP-TSABE scheme

In this scheme [1] the author has described a model for fine grained Access control in Cloud Mainly based on Time frame based access control including self destruction after a specific time and private key encryption. In the system main attention is given to the fact that since a full lifecycle privacy solution is not possible or rather we should say it is very difficult, we are using a method in which the confidential data is to be secured for a specific time period because it can be accessed in that specific time interval only. In this scheme a self destruction mechanism is also added through which the data which is not of use after a specific period of time is destroyed automatically.

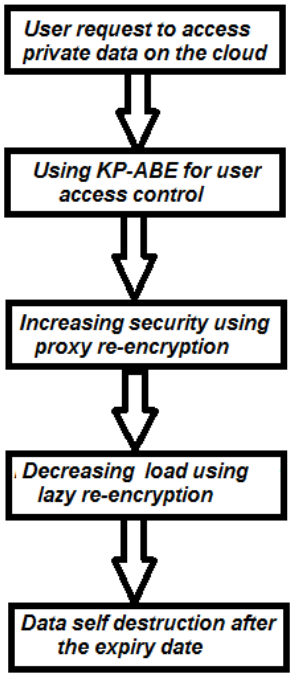
Block Diagram of KP- TSABE



System model of advanced KP-ABE scheme

In this scheme [2] the author has proposed a system which is primarily base upon the KP –ABE scheme in which two new concepts are being merged i.e. Proxy re-encryption and Lazy encryption. In the proposed system the major focus is given on the security of the data and the computational load on the systems to allow or disallow the data access. The security of the system is enhanced using the Proxy re-encryption in which the public key can be transformed into another public without bothering the actual data. And the computational load of the system is reduced by using the lazy re-encryption is used in using some dummy attributes we reduce the computational load on the system.

Block Diagram of advanced KP- ABE



After going through both the methodologies for Fine grained Data access control in cloud computing we have formulated the an analysis report which compares two separate researches for Fine grained Data access control in cloud computing that are KP-TSABE and Advanced KP-ABE. Our analysis is based on the four parameters selected that are **Confidentiality, Encryption, Computational load, Memory utilization** and **Complexity**.

Confidentiality: When we talk about our confidentiality both KP-TSABE and advanced KP-ABE perform well in that context. In confidentiality KP-TSABE is a bit better in comparison with advanced KP-ABE because it not only uses encrypted keys but also the time frame access control of the user data.

Encryption: Talking about our encryption both KP-TSABE and advanced KP-ABE perform well in that context also. In encryption KP-TSABE is a bit better in comparison with advanced KP-ABE because it uses proxy re-encryption in addition to the base encryption where as advanced KP-ABE uses only base encryption.

Computational Load: In Comparison of computational load KP-TSABE takes lead over KP-ABE. In computational load KP-TSABE is a bit better in comparison with advanced KP-ABE because of the lazy re-encryption technique in KP-TSABE and whereas advanced KP-ABE is based on time frame control technique.

Memory utilization: In terms of memory utilization both KP-TSABE and advanced KP-ABE have got some big differences. In memory utilization advanced KP-ABE is better in comparison to KP-TSABE because in advanced KP-ABE the data is deleted itself after the use i.e. it has self deletion whereas nothing such happens in KP-TSABE.

Complexity: In case of complexity Advanced KP-ABE is better because it does not use or require any proxy re-encryption or lazy re-encryption as in case of KP-TSABE.

IV. CONCLUSION

Both KP-TSABE and advanced KP-ABE are high quality fine grained Access control techniques, but after making the comparison of the two on the basis of four selected parameters that are **Confidentiality, Encryption, Computational load, Memory utilization** and **Complexity**. Advanced KP-ABE proves to be more efficient in controlling the scenarios that came across our analysis. Detailed analysis reveal that both the techniques are very good at as both of them add special features in their working to reduce computational load and overhead whereas enhance User security using latest and efficient encryption system. Even though the difference by which advance KP-ABE is very small but when compared it take a very slight edge over KP-TSABE.

REFERENCES

[1] Jinbo Xiong, Ximeng Liu, , Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen. “A secure data self-destructing scheme in cloud computing ”. 2014. IEEE TCC

[2] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing ". 2010. IEEE INFOCOM

[3] Bhagyashree Ambulkar and Vaishali Borkar,"Data Mining in Cloud Computing", MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April 2012.

[4] Peter Mell, and Timothy Grance,"The NIST Definition of Cloud Computing", the National Institute of Standards and Technology, USA, 2011.

[5] ORACLE, "Oracle Data Mining Mining Techniques and Algorithms"

[6] M.Kantardzic, "Data Mining: Concepts, Models, Methods and Algorithms", John Wiley & Sons Inc., 2002.

[7] "Introduction to Cloud Computing Architecture", Sun Microsystems, 2009.

[8] "Top 10 Algorithms in Data Mining", Springer-Verlag London Ltd., 2007.

[9] Jianzong Wang,Zhuo Liu, Peng Wang,"Data Mining of Mass Storage Based on Cloud Computing".

[10] M. Bramer. Principles of Data Mining. Springer, 2007.

[11] M. Brantner, D. Florescu, D. A. Graf, D. Kossmann, and T. Kraska. Building a database on s3. In J. T.-L. Wang, editor, ACM, pages 251–264, 2008.

[12] S. H. Brown. Multiple linear regression analysis: A matrix approach with matlab. Alabama Journal of Mathematics, 2009.

[13] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control Pages 85–90, 2009.

[14] C. Clifton and D. Marks. Security and privacy implications of data mining. In ACM SIGMOD Workshop, pages 15–19, 1996.

[15] Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices. In: 41st ACM Symposium on Theory of Computing, May 31-June 2, 2009, Bethesda, Maryland, USA, pages 169–178 (2009) Boneh, D., Goh,

[16] E-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Proceedings of TCC 2005, volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)

[17] Lindell, Y., Pinkas, B.: Privacy Preserving Data Mining. J. Cryptology 15(3), 151—222 (2002) .Liu, K.: Privacy Preserving Data Mining Bibliography

