MEASURABLE, SAFE AND SECURE DATA MANAGEMENT FOR SENSITIVE USERS IN CLOUD COMPUTING

Pallaty Babitha[1], Ravi Mathey[2]

[1]*M.Tech, student [Computer Science Engineering], Vidya Jyothi Institute of Technology*
[2]*Head of the Department, Vidya Jyothi Institute of Technology*

Abstract

Cloud Computing is most trustworthy internet paradigm for small scale business entrepreneurs. The increased use of cloud computing applications has grown the users access to the database. The increase usage of users access has created the privacy problems in cloud computing. The increased usage of data centers with different users has given rise to data leakage and privacy data issues. The data owner could not trust the users access as the data of other users is accessed and revealed to other users. There is an urgency to arrest the problem of privacy issues and data security. The proposed project is developed to support the delegation of private keys to the users. This private key is generated to subsumes Hierarchical Identity-Based Encryption. The proposed project is developed on the basis of attribute based access rights to the users from the data owner. The project is developed to convey the protected key through automatic mail as soon as the user is registered with the data owner for accessing the fine-grained data sharing.

Keywords: *Cloud Computing, Data Access, Attribute Based encryption and Decryption.*

----------***----------

1. INTRODUCTION

Cloud computing is one of the most trusted business paradigm for small and medium scale entrepreneurs with unlimited resources with most economical range in the internet. Cloud computing is facilitating Software as a Service, Platform as a Service, Infrastructure as a Service and Database as a Service. Cloud computing is distinguished as the best providers for infrastructure as a service and database as a service. Cloud Computing is provided by big data server operators. Small and Medium scale entrepreneurs are using the services [IaaS, PaaS, DBaaS, SaaS] of cloud computing. The cloud service providers are facilitating the cloud servers to the Cloud Consumers. The cloud consumers have their own customers. The Cloud consumers are using cloud computing servers for data sharing and sharing of sensitive data with the customers. The cloud users are using the cloud services for their operations. The cloud users will store the data and share some sensitive data to their customers. The operation should be done in safe and secure manner with prescribed quantity of data to the distinct users.

The present paper is focusing on sharing the sensitive data preserved in cloud computing to the distinct users in a safe and secure manner. Every user will be given permission to access a limited and prescribed amount of data which belongs to a specific period only. The user can't view and access all the data available in the remote servers. To perform this operations user profiles are created and user access rights will be generated for the every user by the administrator. This limited and prescribed amount of data has to be accessed by the specific user. This has to be done with great confidentiality and access permissions to the users who wants to utilize the data. In this project user permissions and access rights are playing predominant role. In this project a novel encryption method to access a measurable data for a specific user or for a specific user profile.

2. BACKGROUND WORK

The Background of the project is to illustrate the cloud computing security issues.

2.1 Cloud Computing Data Storage

In the research study the most important point to be considered is data storages in cloud computing. In this concept several papers have been studied and properly investigated. In fact the cloud computing has problems with data storage. Many cloud computing consumers have been accessing the cloud servers. The cloud servers have been used by the users of the cloud computing consumers with huge amount of data storage. At this juncture the data belongs to one cloud consumer users have been mixed up with the other cloud computing consumer data. This has been the scenario to reveal the privacy of one cloud computing consumer data to the other cloud computing consumer. The immediate admeasure is essentially needed to preserve the data confidentiality to the cloud computing data storage. . [Trend Micro][2]

2.2 Secure Data Access

Fuzzy keyword search over encrypted data is another finest project to be considered. In this project the project team has focused on the quantification of key words and development of advanced key words sets for better identification in the database servers. In this project the process has preserved the data privacy in cloud environment. For this the process has implemented fuzzy keyword search to increase the system usability and also revealed only files which are matching with the specific search for revealing the related data for the users. In this research work the private matching is also taken into consideration to secure multiparty computation for data privacy in the servers. The fuzzy key word search scheme provided the data owners the safe and secure data management in the cloud servers. This project has discussed the threat model and design of goals to attain the safe and secure data access in cloud servers.[Jin Li, Qian Wang][3]

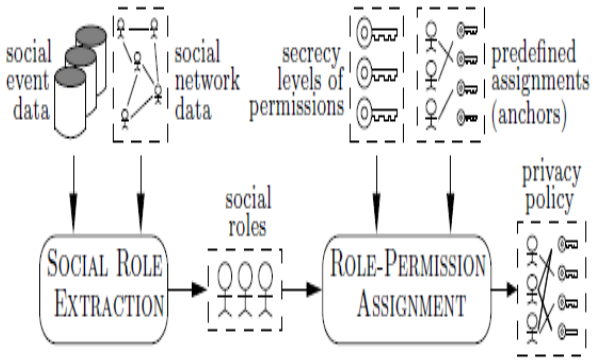

Fig: 1 Attribute Based Encryption methods for safe and secure social event data

3. EXISTING SYSTEM

The existing solutions are rich with data revealing with the help of cryptographic methods for authorized users. Authorized users can achivew all sensitive and public data in the existing system.

3.1 LIMITATIONS

- In existing system data owner of cloud computing server cannot manage the distribution of fine grained data to specific users.
- At the same time measurable data access, data confidentiality and control over data is not addressed in the existing system.
- In an existing system solution is flexible, but it is vulnerable to collusion attack.

4. PROPOSED SYSTEM

The present project is focusing on sharing the sensitive data preserved in cloud computing to the distinct users in a safe and secure manner. In this project all customers [users] should not access all the data of the company [cloud consumer]. Every user will be given permission to access a limited and prescribed amount of data which belongs to a specific period only. The user can't view and access all the data available in the remote servers. To perform this operations user profiles are created and user access rights will be generated for the every user by the administrator. This limited and prescribed amount of data has to be accessed by the specific user.

4.1 Advantages

- The project is addressing existing problems in cloud computing data distribution of fine grained data.
- The present system is incorporating the access policies on the basis of data attributes. The data owner can give access rights to specific users on the specific fine grained data.
- The project is rich with Attribute Based Encryption technique, proxy re-encryption method and lazy re-encryption techniques to achieve the measurable and fine-grained cloud computing data management.
- To get measurable fine grained data access control the proposed project is enriched with cloud computing system models, cloud servers security models, user accountability, user permission granting and revocation of permissions with one-to-many communication systems.

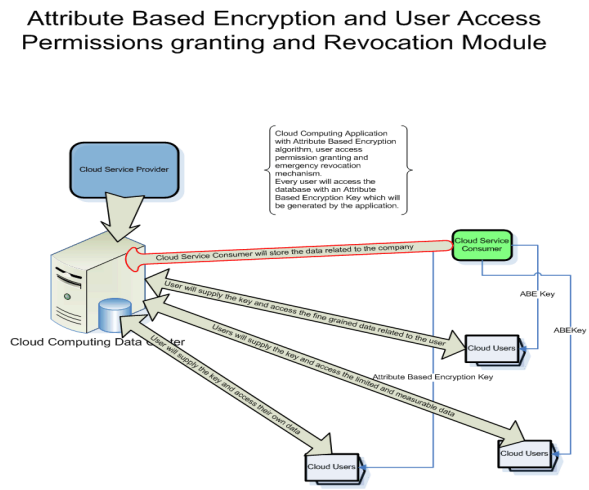

Fig 2: Access permissions

4.2 Critical Analysis

The project is a simulation project. The project is describing the user access with safe and secure mechanism. The application is developed in .Net technologies. The application is replicating the cloud computing environment with cloud service Providers, Cloud users [Cloud Consumers] and Cloud users. The project is developed with three modules. Cloud service providers will provide the cloud server to the cloud consumers. The cloud consumers will hive the server space and store the data in the database residing in cloud servers. The Cloud Consumers have customers. The customers should access the relative data from the cloud consumer data. The cloud consumer will store the data in the cloud server hence the cloud consumer

will be regarded as data owner. Whenever the cloud users [customers of cloud consumers] wants to access the relative data, the data owner will permit the cloud user to access the specific data related to the users. To permit the users to access the relative data, the cloud consumer [data owner] will incorporate a mechanism to give user access permissions to the users. This mechanism is rich with attribute based algorithms.

5. IMPLEMENTATION

The implementation of the project is done in .net frame work and working with IIS server environment. IIS server is replicating the cloud environment and the users and cloud consumers and cloud service providers will perform their duties accordingly. The implementation of the project is done in IIS server and with the configuration of host for the web based application. The application should be accessed by different systems connected in LAN. The application will be implemented in the web server which consists of IIS server.

The cloud owner should access the web based applications residing in the web server and store the data in the database tables. The data inserted into the database tables are belonged cloud users. The cloud user will be given access permission by the cloud consumer. The data will be accessed by the users from different computers in LAN. In this way the cloud computing architecture can be demonstrated in the simulation environment. In fact the application what is intended to access by the users can be deployed in the cloud servers and use the relative database. But it can be treated as the cloud real time environment.

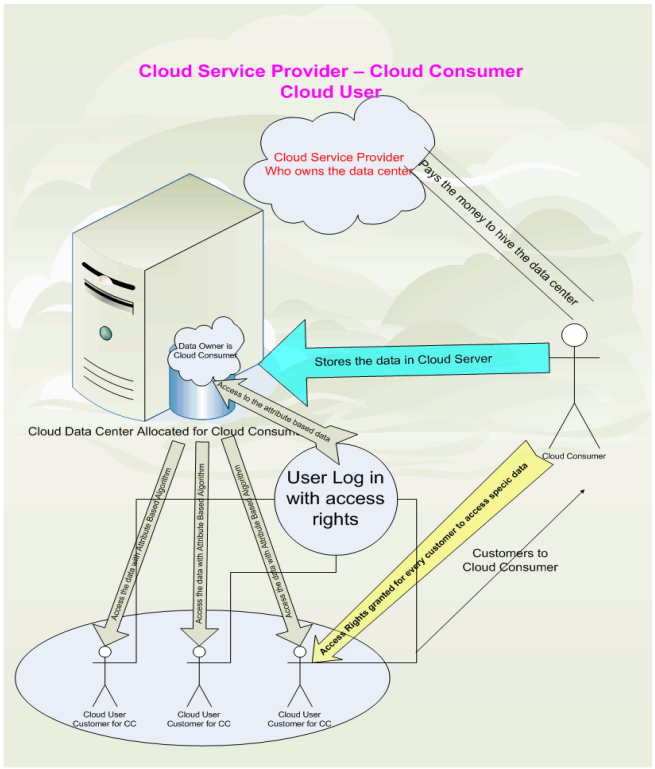

Fig 3: System Architecture

6. RESULTS

The results of the project can be revealed by the output of the project. The output of the project is allowing the users to access their own data depicted in the database row. The database row demonstrate the details of the users of cloud consumers. Hence the result is to access the specific row by the user. This mechanism is achieved by the project executor with the help of attribute based algorithms. The project is developed with the combination of attributed based algorithms as well as user access permissions to the users for the specific row of the table.

The result is revealed as soon as the user could access his own data from the database. In addition to that the database access rights should be given by the cloud consumer. This mechanism is depicted in the project. The results evaluation has revealed that the data accessed by the client will be limited to the data related t the client. This has achieved in the project with the help of attributed based algorithms and user access rights and revocation grants to the users to access the specific data. The results have revealed that creating the cloud computing environment in the Micro soft visual studio and SQL server with in the frame work of .Net. The database is SQL server.

7. CONCLUSIONS

Cloud computing has grown up with its virtues. At the same time the cloud computing is also declined with the flaws. The project is trying to reduce the privacy issues and security threats in the cloud computing. To provide the privacy preserving techniques the attribute based algorithms and user access permission have been implemented to achieve the best results in cloud computing privacy preserving methods. The project has successfully implemented in . Net framework and the front end- web based screens have developed with visual studio tools. SQL Server Database has implemented to store the data by the data owner. The data pertaining to the cloud users have been accessed with limited and specific orientation as permitted by the data owner. The project has successfully in the client server architecture in LAN environment. The user could access the relevant data as permitted by the cloud consumers.

FUTURE SCOPE OF STUDY

The future scope of the project is done with the real time environment. The application whatever we have deployed in the IIS server should be implemented in Internet Service Providers space and run the same to reveal the results.

The future scope of the project is unlimited. The cloud computing is one of the best trusted business. But in the recent years the flaws and privacy issues have degraded the business of cloud services to the customers. The future scope of the study should be developed to identify the flaws of the cloud computing and give proper solution to the cloud computing in the combination of Digital Forensic details,

and to show the cloud computing operations as trust worthy for operating anything.

REFERENCES

[1] Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing by Shucheng Yu, Cong Wang, KuiRen and Wenjing Lou

[2] SecureCloud™ Securing and Controlling Sensitive Data in the Cloud by Trend Micro

[3] Fuzzy Keyword Search over Encrypted Data in Cloud Computing by Jin Li, Qian Wang, Cong Wang, Ning Cao, KuiRen and Wenjing Lou

[4] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proceedings of Crypto 2007, volume 4622 of LNCS. Springer-Verlag, 2007.

[5] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE Symposium on Security and Privacy'00, 2000.

[6] E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, Report 2003/216, 2003, http://eprint.iacr.org/.

[7] Amazon Web Services (AWS), Online at http://aws. amazon.com.

[8] Google App Engine, Online at http://code.google.com/appengine/.

[9] Microsoft Azure, http://www.microsoft.com/azure/.

[10] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[11] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.

[12] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002.

[13] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data by VipulGoyal, OmkantPandeyyAmitSahaiz and Brent Waters.

[14] Fine-Grained Access Control of Personal Data by Ting Wang, MudhakarSrivatsa and Ling Liu

[15] Fine Grained Access Control by Arup Nanda, Proligence, Inc.

[16] Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control by Richard Chow, Philippe Golle, Markus Jakobsson, RyusukeMasuoka, Jesus Molina

[17] A Synchronization Algorithm of Mobile Database for Cloud Computing by Ranjeet Singh and ChiranjitDutta - Volume2 Issue3 March 2013.International Journal of Application or Innovation in Engineering & Management (IJAIEM)

[18] To enhance multimedia security in cloud computing environment using crossbreed algorithm by SonalGuleria and Dr. Sonia Vatta taken from International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 6, June 2013.

[19] Using Data-Oblivious Algorithms for Private Cloud Storage Access by Michael Goodrich article published on Thursday, October 24th, 2013 10:30 am – 11:00 am downloaded from http://simons.berkeley.edu/talks/michael-goodrich-2013-10-24.

[20] Using encryption Algorithms to enhance the Data Security in Cloud Computing by MANDEEP KAUR and MANISH MAHAJAN [2013] published in International Journal of Communication and Computer Technologies.

[21] A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture by KawserWazed Nafi1,Tonny ShekhaKar, SayedAnisulHoque, Dr. M. M. A Hashem published in) International Journal of Advanced Computer Science and Applications,year 2012.

[22] Capability-based Cryptographic Data Access Control in Cloud Computing by ChittaranjanHota, Sunil Sanka, MuttukrishnanRajarajan and SrijithK.Nair. Published in the year 2011.

[23] Database security in the cloud by ImalSakhi Published in 2012

[24] Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings by Ming Li, Shucheng Yu, KuiRen, and Wenjing Lou published in Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010.

[25] Mohamed Sami [2012] Personal website – Software Engineering Practices downloaded from http://melsatar.wordpress.com /2012/03/15/ software-development -life-cycle -models -and-methodologies.

BIOGRAPHIES

1. P.Babitha is M.Tech Student at Vidya Jyothi Institute of Technology (VJIT).

2. Ravi Mathey is a post-graduate specialized in Computer Science from BIT -Ranchi and he did Instrumentation technology in Andhra university. He has more than 20 years of experience in Research and Development, and teaching Presently he is working as Associate Professor and HOD of CSE Department at Vidya Jyothi Institute of Technology (VJIT). His area of research is wireless embedded application and image compression techniques by using fractals and wavelets, cloud computing