Data management with Attribute Based Encryption method for sensitive users in Cloud Computing

Vidyasagar Tella, L.V.Ramesh

***Abstract*— Cloud Computing is known as the most affordable internet paradigm for small scale business entrepreneurs. The pricing and services provided by Cloud Computing are very attractive and useful for small and medium sized enterprise owners to perform their operations in desired application. The increased usage of cloud computing has given opportunities for hackers to steal sensitive data from the database of other institutions. To stop the eavesdropping activities of hackers and virus producers, a secure data management has been developed and introduced in this project. The cloud users who is managing his enterprise will hive the services of cloud computing and store the data into cloud servers. The data owner will have customers of his enterprise will enable the customers to access the relevant and relative data. To give access to the relevant data, the present novel concept has been developed and introduced in the field of cloud computing. This concept is developed to allocate private keys to the users. This private key establishes the Hierarchical Identity-Based Encryption. Attribute based access rights to the users can be incorporated by the data owner in this project with required security scheme. So that the data owner can keep the data of all customers and only relative data can be accessed by specific customer related to specific data.**

***Index Terms*— Cloud Computing, Data Access, Attribute Based access rights..**

I. 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.

Manuscript received September 23, 2014.

Vidyasagar Tella, Pursuing M.Tech Computer Science Engineering Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh

L.V.Ramesh,Assistant Professor, Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh

II. BACKGROUND

The Background of the project is to illustrate the cloud computing security issues. In this project the cloud computing security has been incorporated with attribute based encryption algorithms and access rights mechanism from cloud computing consumers to its customers. The project is rich with the following salient features.

The project is rich with Attribute Based Encryption, proxy re-encryption and lazy re-encryption to achieve the measurable, safe and secure cloud computing data management. To get the measurable fine grained data access control the proposed project is enriched with cloud computing system models, cloud servers security models, user accountability, user grant / revocation permissions and one-to-many communication systems.

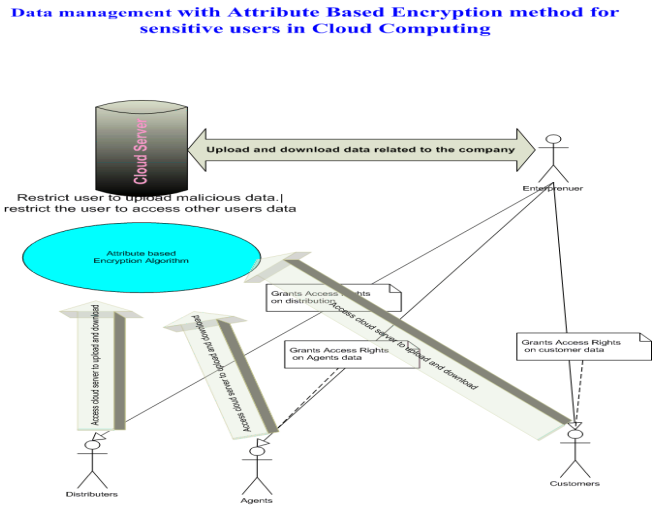
The preliminary techniques like key policy attribute-based encryption, cryptographic primitive with semi-trusted proxy to convert cipher text and Lazy re-encryption with set of attributes data file.

III. 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. 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. This experimental operation

is configured in cloud environment for the users related to the specific user set of data are incorporated.



IV. CRITICAL ANALYSIS:

Data management in cloud computing with safe and secure operations is predominant task of the project. The project is rich with granting user access to the specific users of the enterprise owner and apply the attribute based encryption algorithm to restrict the user to access unwanted data and upload malicious data.

The combination of two methods in creating the users and giving access permission to the database made the project to consider as the best database management project in cloud computing with proper security.

The project is developed to implement necessary security measures for the accessing the database for retrievals and storage. The project method is predominant to restrict the users to upload the malicious data.

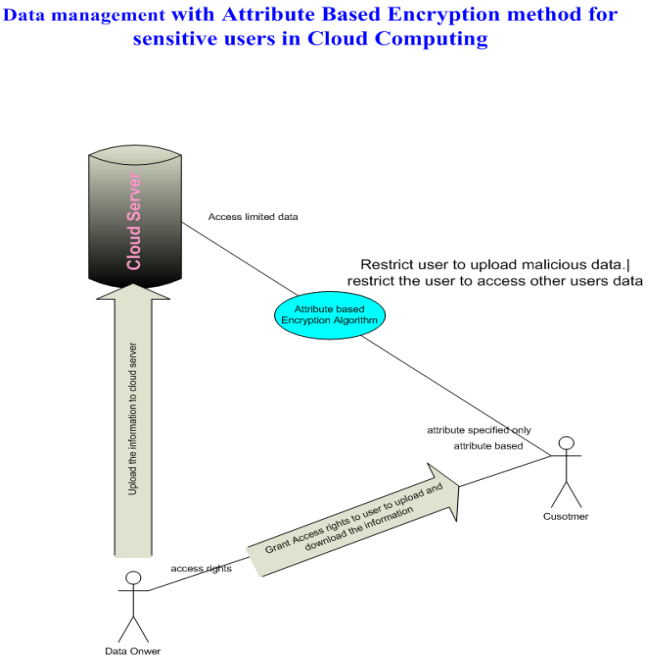
The project is developed to implement necessary privacy preserving point to safeguard the data belongs to other users. This project prevents the user not to access the data which did not belongs to him or her.

This project has implemented all international standards of code behind the technique to incorporate the above said mechanisms.

The project is designed and developed in visual studio with .Net framework to exemplify the cloud operations in the simulation environment.

V. IMPLEMENTATION

The implementation of the project is done in .net frame work. The project is running in the IIS server to exemplify the cloud 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.



VI. RESULTS

The output results have been evaluated. The evaluated results have revealed that the implementation attribute based access right has incorporated the attribute based access the relative data of the customer. The row or specific column of data can be called as attribute. The present project enable the user to access a specific attribute allocated by the data owner of cloud consumer. The data management with safe and secure access to the user has been established by using the attribute based encryption method successfully done in this project. The project is rich with attribute based encryption method as well as the granting specific attribute access rights to the user would be the predominant mechanism.

The results have obtained as soon the data is stored in the server.

The results have been obtained as soon as the user is created.

The user has been granted access rights to a specific row or column.

The access policy will be mailed to the specific user with the user name and password.

The user will be performing the access of the data through the attribute based encryption method.

Different users are permitted to access relative and corresponding data available from the pool of rows of the database.

The results have obtained from uploading option also. In the uploading options any data is infected with virus, the attribute based access rights will restrict the data to upload the file into the server.

The data management with attribute access rights and user access rights have restricted the users to interact with the server to upload any malicious data.

The cloud computing environment has been created with the help of SQL Server 2008 database and .Net framework. The attribute based encryption algorithms and access rights code behind the technique has been designed and developed using ASP.Net, C#.Net and ADO.Net.

The project goal has fulfilled by incorporating the code behind the technique in creating attribute based access rights and granting the access to the users with specific attributes.

VII. 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. In this juncture the results would be revealed by the users should be revealed to the cloud consumer in a separate screen or form.

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. The future scope is to show the cloud computing operations as trust worthy for operating anything.

VIII. Conclusion

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.

Reference

[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.