International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Expressive and Deployable Dynamic Query Forms of the Database in Cloud Secure Environment

P.Boobalan[1], S.Dharshini[2], A.Sheebha Christiana[3], K.Aravindhan[4]

[1]Associate Professor, [2,3,4]B.Tech
[1,2,3,4]Department of Information Technology, Pondicherry Engineering College, Puducherry, India
[2]dharshinisekar123@gmail.com, [3]sheebhachristiana@gmail.com, [4]aravindhanking61@gmail.com

Abstract: Cloud computing is an emerging computing technology that enables user to store data into the cloud server to improve scalability and on-demand services. Not all cloud providers are trustworthy. To protect data privacy against untrusted cloud service providers, existing solution apply cryptographic methods. However, sharing cloud data among authorized users is still a challenging issue, especially when dealing with dynamic user groups. In this paper, we propose a secure access control by creating dynamic query forms according to the roles of the user in cloud environment. We use Light Weight Symmetric Encryption Algorithm. This algorithm aims at encrypting the data in the database and encrypts all forms of queries without any changes in the database structure. By creating dynamic query forms, there exits privacy in the data that is stored in the cloud.

Keywords: Light Weight Symmetric Encryption Algorithm (LWSEA), Dynamic query forms(DFQ).

1. INTRODUCTION

The main objective of this project is to create dynamic query forms according to the roles of the users in cloud environment using Light Weight Symmetric Encryption Algorithm. This algorithm aims at encrypting the data in the database and encrypts all forms of queries without any change in the database structure. This process comes under the technique of Role Based Access System. This project aims at creating dynamic query forms of the database using the dynamic query forms, which will give the result of the related activities of the user. By creating dynamic query forms, there exists privacy in the data that is stored in the cloud.

The users who are trying to access the pages or files to which they lack access permissions, are blocked and will not be permitted to access any of the files in the cloud. Consider a practical application that a company allows its staff or department to store and share data via a cloud. By utilizing the cloud, the company can be completely released from the local storage and maintenance burden. However, it also incurs a major security threat towards the data confidentiality. To address this issue, a basic solution is to encrypt data and then upload the encrypted data into the cloud.

Another threat faced by the company by utilizing cloud storage is unauthorized user accessing the files that are stored in the cloud storage. This problem is also addressed in this paper. The user who are trying to access the pages or files, to which they lack permissions, are blocked and will not be permitted to access any of the files.

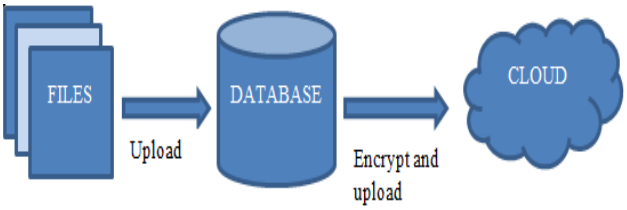

Figure 1. General mechanism of cloud storage

2. DATABASE

We have not found a widely used or publically available database of an organization or a company. So we decide to create a new database on our own. We created a nearly 100 entries in the database. The database can be created in any software available like MySQL, Oracle and Microsoft Access.

3. LITERATURE SURVEY

In table1.1 various encryption algorithm and techniques have been compared with their respective advantage and disadvantage.

Table 1.1 Comparative studies on various existing encryption algorithms techniques.

Sl. No	Name of the journal, Year	Title of the paper	Algorithm	Dataset used	Parameter	Results	Limitations
1.	IEEE Transaction on dependable and secure computing, 2019	Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud	Onion encryption algorithm	Real world data set	Achieve higher efficiency in access revocation	Encryption for each layer increase	Number of bits used for encryption is very less, which makes the data prone to attacks.
2.	IEEE Transactions on Information Forensics and Security, 2018	Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud	Revocable attribute based encryption	On-demand movie streaming system	Better efficiency has been achieved which reduces workloadof service provider.	Allows to update cipher text for handling revocation	It doesn't allow the practical revocation of malicious or expired users.
3.	Elseiver Transaction,2017	LEncDB: lightweight framework for privacy-preserving data queries in cloud computing	LWSEA algorithm	Plain text, SQL statements-input Encrypted SQL statements-output	Execution time	This method is effective and be applied to big database and privacy-preserving application	It faces storage problems due to massive dynamic information.
4.	IEEE Transaction on international conference on Anti-cyber-crimes, 2018	Preventing And Securing Data From Cyber Crime Using New Authentication Method Based On Block Cipher Scheme	Block cipher scheme	Arbitrary data (text and extended integers)	It encrypts and decrypts the data very fast and secure.	It provides data confidentiality,Data authentication and data access control.	Low efficiency in terms of storage requirement for encrypted data.
5.	IEEE Transaction on information and forensic security, 2018	Normal cloud model-based algorithm for multi-attribute trusted cloud service selection	Algorithm of multi granular standard trust cloud	Gaussian distribution X>number of trust values-i/p Gaussian cloud model-o/p	Provides same cloud services with the maximum and minimum trustworthin-ess.	QoS of clouds services are measured accurately	There is no internet based service sharing platform together the real service selection

International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

4. MODEL DESIGN

We have the following steps in providing privacy and security to the files in the organization.

- Creation of different menus
- Preparing ranked list of query
- Assigning query forms as per user role
- Storing data in database
- Encryption of data in database
- Storing in cloud storage.

Creation of different menus: This method includes creating of different menus for the admin , provide page visibility to different users.

Preparing ranked list of query: This method uses a search engine called Dynamic faceted search engine. It is used to make the ranked list of query from which the top ranked query form will be assigned to that specific user.

Assigning query forms as per user role: the top ranked query form will be assigned to the user. The user provides the feedback about the query results. Again the user will be given another query form from the ranked list of query.

Storing data in database: Once the user is assigned with a role he/she can start accessing their files. They can also save their files in the database for further processing.

Encryption of data in database and storing in cloud storage: The data stored in the database will get encrypted and the complete database is stored in the cloud storage. The data is encrypted using LWSEA algorithm.

5. PARAMETERS

The parameters used are

- **Response time:** Response is the time taken to block the user with no accessibility. It is minimized in our proposal.
- **Throughput:** Throughput is the amount of files uploaded in the cloud. One can also upload the bulk data into the cloud storage in our proposal. Throughput is increased to improve efficiency of cloud storage.

6. CONCLUSION

Thus in this paper we have proposed a encryption algorithm that provide a security over the data stored in the cloud and dynamic query form method to provide privacy among the users. Motivated by this problem, we have created a virtual database of an organization. A practical implementation of this technique has not done by any organization hence it can be implemented in upcoming years.

REFERENCES

[1] Qi, Saiyu, and Yuanqing Zheng. "Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud." *IEEE Transactions on Dependable and Secure Computing* (2019).

[2] Kuppuswamy, P., Banu, R., & Rekha, N. (2017, March). “Preventing and securing data from cybercrime using new authentication method based on block cipher scheme”. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 113-117).IEEE.

[3] Luo, W., Hu, Y., Jiang, H. and Wang, J., 2018. “Authentication by encrypted negative password”. *IEEE Transactions on Information Forensics and Security*, *14*(1), pp.114-128.

[4] Xie, Qi, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, and Liming Fang. "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model." *IEEE Transactions on Information Forensics and Security* 12, no. 6 (2017): 1382-1392.

[5] Wang, D. and Wang, P., 2016. “Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE transactions on dependable and secure computing*, *15*(4), pp.708-722.

AUTHOR BIOGRAPHY

Dr.P.Boobalan

He has obtained Master of Technology in Computer Science and Engineering and Ph.D. in Computer Science and Engineering from Pondicherry University. He is an Associate Professor of the Department of Information Technology in Pondicherry Engineering College, Puducherry, India. He is a life member of Indian Society for Technical Education(ISTE).

S.Dharshini

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.

A.Sheebha Christiana

She is pursuing her B.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.

K.Aravindhan

He is pursuing his B.Tech degree in Department of Information Technology, Pondicherry Engineering College, Pondicherry.

