Provide Privacy of Independent Data Access in Cloud Computing

TirumalaRao Gurubelli[1], V.Laxmi Prasad[2]

Final M.Tech Student[1], Asst.professo[2]

[1,2]*Dept of CSE, Sarada Institute of Science, Technology andManagement (SISTAM),*

Srikakulam, Andhra Pradesh, India

***Abstract**:*

In cloud context storing data into cloud is a critical problem for providing security of that data. So to protect that stored data from the untrusted parties place an important role. So that to provide security of that database we are encrypt the database and stored into cloud. Before encrypt the database the group key manager will generate secret key for all group members and sent to all. After sending the group members will encrypt and decrypt the database using that secret key. In this paper we are proposed shared binary transpose protocol for generation of group key and to encrypt, decrypt the databases using rijndael algorithm. By implementing those techniques we can provide more efficiency and privacy of accessing cloud database.

Keywords: *Cloud Computing, Cryptography, confidentiality, database, security.*

I. INTRODUCTION

Now a day's storing critical information placed into cloud computing is a untrusted infrastructure of third parties. By storing information into the cloud should provide more confidentiality of that information. So that to access that information only by the trusted parties, that information not accessible other parties of cloud services, untrusted third parties and internet. To provide security of stored data from the untrusted third parties by performing cryptography technique. By implementing cryptography technique we can encrypt the stored database and stored into cloud computing. Now a day's so many solution are available for providing confidentiality database. By implementing confidentiality of database is still open research area. In this type of context we can proposed one of cryptography technique for provide security of database. By implementing these concepts we provide more efficiency of database and also provide reliability without exposing unencrypted data to the cloud service provider.

The architecture design mainly contains two types of concepts. By implementing this architecture to allow multiple parties can be shared information through cloud and also provide more security of transferring information. By performing confidentiality of storing database we can perform the encryption process of cryptography technique.
In this paper we are implementing information sharing can be done by client, to eliminate intermediate parties. The possibility of combining the security and availability cloud database we can implementing encrypted database from many geographically distributed clients in cloud computing. To achieve security and availability secure database integrate some of the existing cryptography technique. By implementing cryptography technique we provide security of untrusted third parties in the cloud database. In this paper contains implementation procedure for cryptography and generation of secret key for the trusted third parties. By the implementation point of view we can't apply typical implementation procedure.

In this architecture we are implementing secure data base of cloud platform and does not provide any intermediate third parties in this architecture. To eliminating intermediate parties we can provide more availability and reliability of cloud database. To maintaining third parties in the cloud computing will face the problem of single point failure and bottleneck that limits availability and reliability of cloud database. Unlike by implementing this architecture the client will perform the read and write operation on database is directly and also face the problem of modification of data structure. By implementing this architecture in a large set of real world cloud computing platforms will be demonstrated that security of database will be applicable immediately. By implementing this architecture we can improve the efficiency of network for read and writing of data into cloud.

By implementing direct accessing database from the cloud we can provide availability of data and also provide security of cloud database. So that each client we can directly get information from the cloud database with secure manner. In this architecture we can also provide modification of cloud database can be done by client. In this context each client can be performed cryptography concept

for data encryption and decryption.The motivation of these results is that network latencies, which are typical of cloud scenarios, tend to mask the performance costs of data encryption on response time. The overall conclusions of this paper are important because for the first time they demonstrate the applicability of encryption to cloud database services in terms of feasibility and performance

The remaining parts of this paper are as follows: 2. related work of this paper 3. Implementation procedure of proposed system
4. Result analysis of proposed system 5. Conclusion of proposed system 6. Reference can be used by the proposed system

II. Related Work

To provide security of data several features differentiate it from the previous work in the fields to provide the security of cloud database.To provide confidentiality of data in the cloud to concurrently perform the reading and writing operation of encrypted data. So that by performing the concurrent reading and writing operation on cloud data we provide availability and scalability of cloud database. Because it does not require any intermediate servers so that response time of the request will come very fast. By implementing this architecture multiple clients can distribute and independent access the cloud database. Another advantage is that does not require any trusted centred because the stored data in the cloud must be a in the form of encrypted format. By implementing the security of data we using cryptography file system and secure storage solution will represent earliest work in the field.

Now a day's to provide security of data different approach can give the confidentiality of distributing data among different providers and by taking advantage of secret sharing [2]. By performing secret sharing of data in cloud we can provide one of cloud provider in the cloud computing. So that by implementing this type of architecture we can face the problem of maintain intermediate proxy servers. So that this problem can be overcome by implementing the proposed system. To provide security of data in cloud we cannot use multiple servers for sharing of data the network. The security of data close related to encryption process for protecting the cloud data from the untrusted users. To perform the security of cloud data by using one of cryptography technique can directly apply the plain data.

Some of the data cryptography techniques offer different types of encrypted data for transferring data form one format another format. To perform the transferring data from one format another format by using encryption process in the cryptography technique [3][4]. The conversion process plain text to unknown format data is called the cipher text. The conversion cipher format to plain format is called the decryption process in the cryptography technique. By implementing this feature the trusted users can get data from the cloud. Some of the other [5] solution also available for the performing operation of encrypting the cloud data. By implementing these approaches we can provide confidentiality of data in the scenario of trusted users. However to provide security of data in cloud some of the cryptography standards are available in the network security. For this reasons security of data related [9]to [8] that preserve the confidentiality of cloud data from the untrusted users. However by overcome these problems we can maintain the intermediate servers by performing interaction between the client and cloud servers. So that by implementing this approach we can perform the block the data instead of each data item. Whenever the data item is related to block data, the trusted users will retrieve whole block and perform the encryption process. After performing the encryption process we can perform the same block decryption process we can get original block of plain text.

The character and implementation of secure data and is applicable to multi-tier web application that is main focus of our web application. By implementing this architecture it causes the several draw backs. If the information is sharing in the cloud it must be trusted users and its function cannot be outsourced to untrusted parties.Hence, the proxy is meant to be implemented and managed by the cloud tenant. Availability, scalability, and elasticity of the whole secure Data service are then bounded by availability, scalability, and elasticity of the trusted proxy, that becomes a single point of failure and a system bottleneck. Since high availability, scalability, and elasticity are among the foremost reasons that lead to the adoption of cloud services, this limitation hinders the applicability of [6] and [7] to the cloud database scenario. Security of data solves this problem by implementing of the client direct connect with cloud database, without need of any intermediate server of cloud computing.

By implementing this architecture we cannot maintain the intermediate server in cloud. So that the client will directly access data from the client and also directly store the data into cloud. Before performing store of data into cloud each client will encrypt the data and stored into cloud. After storing the data into cloud the user will retrieve the data from the cloud and decrypt. By performing the decryption process will get original plain format data. Secure data extends our preliminary studies [9] showing that dataconsistency can be guaranteed for some operations byleveraging concurrency isolation mechanisms implemented

in engines, and identifying the minimum isolation level required for those statements.

III. PROPOSED SYSTEM

The proposed system mainly concentrates on independent access of encrypted cloud database. Before access the cloud database each group member will store the database into cloud. So that the group member store cloud database before they are encrypt and store into cloud. Before encrypt the database the group member will generate group key for encryption and decryption of cloud database. The generation of group key they are using shared binary transpose protocol. After generating secret key the group members will encrypt and decrypt the cloud database using rijndael algorithm. The generation of group key is as follows.

Shared binary transpose protocol:

In this module the communication between group key manager and group members. The generation of group key process is follows.

1. Each member sent request for communicating group key manager.

2. The group key manager sent id as respond to each group member.

3. Each group member will choose two prime number is p and g. the group member also choose private key as a.

4. After choosing prime numbers and private key to generate public key by using following formula.

   Pubkey= g^a mod p

5. After generating public keys the group member will send those keys to group key manager.

6. The group key manager takes those public keys and generating secret key by using following steps.

   Xorkey=$pubkey_1$ ® $pubkey_2$ ® ……®$pubkey_n$

   where n is number of group members

   b) convertxorkey value into binary format.
   c) after converting binary format the group key manager will reverse those binary bits.

   Binary=convert(xorkey) to binary format
   Revbits =rev(binary)

   d) After revering binary bits then convert into ascii format.

7. The group key manager will take that value and generate some shared key of Individual group members. The generation of shared key as follows.

$sharedkey_i$=ascii-$pubkey_i$

8.The group key manager will sent those shared keys to individual group member.

9.The group member will retrieve those shared key and generate secret key is as follows

$secrekey_i$=$sharedkey_i$+ $pubkey_i$

After completion of secret key generation each user will encrypt and decrypt the cloud database using this secret key. The process encryption and decryption as follows.

Encryption and decryption cloud database:

In this module each user store the cloud database into cloud. Before store the cloud database each user will encrypt that stored cloud data and stored into cloud. By performing encryption process each user will use rijndeal encryption process. So that completion of encryption process the group member will store the cloud database into cloud. If any user want to particular database they can retrieve and decrypt using rijndeal decryption process. After decryption of cloud database the group member will get plain type of cloud database.

IV. CONCLUSIONS

We propose an innovative architecture that guarantees confidentiality of data stored in public cloud databases. So that in this paper we are propose concept of generation of group key and cryptography technique. For the purpose of generation of group key is to use encrypt and decrypt cloud database using that key. In this paper we are using shared binary traverse protocol for generation of group key. Another concepts for encryption and decryption of cloud database we are using rijndeal algorithm. By implementing those concepts to take full advantage of DBaaS qualities, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider.

V. REFERENCES

[1].B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M.Newbold, M. Hibler, C. Barb, and A. Joglekar, "An IntegratedExperimental Environment for Distributed Systems and networks,"Proc. Fifth USENIX Conf. Operating Systems Design andImplementation, Dec. 2002.
[2]. A. Shamir, "How to Share a Secret," Comm. of the ACM,vol. 22, no. 11, pp. 612-613, 1979..
[3]. "Oracle Advanced Security," Oracle Corporation, http://www.oracle.com/technetwork/database/options/advanced-security,Apr. 2013.
[4] G. Cattaneo, L. Catuogno, A.D. Sorbo, and P. Persiano, "TheDesign and Implementation of a Transparent Cryptographic FileSystemFor Unix," Proc. FREENIX Track: 2001 USENIX Ann. Technical Conf., Apr. 2001.
[5] E. Damiani, S.D.C. Vimercati, S. Jajodia, S. Paraboschi, and P.Samarati, "Balancing Confidentiality and Efficiency in Untrusted Relational Dbmss," Proc. Tenth ACM Conf. Computer and Comm.Security, Oct. 2003.
[6] H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, "ExecutingSQL over Encrypted Data in the Database-Service-ProviderModel," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.
[7] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan,"CryptDB: Protecting Confidentiality with Encrypted QueryProcessing," Proc. 23rd ACM Symp. Operating Systems rinciples,Oct. 2011.
[8] *The gnu multiple precision arithmetic library* [Online]. Available:http://gmplib.org/
[9] L. Ferretti, M. Colajanni, and M. Marchetti, "Supporting Securityand Consistency for Cloud Database," Proc. Fourth Int'l Symp.Cyberspace Safety and Security, Dec. 2012.
[10].A. Boldyreva, N. Chenette, and A. O'Neill, "Order-PreservingEncryption Revisited: Improved Security Analysis and AlternativeSolutions," Proc. 31st Ann. Conf. Advances in Cryptology (CRYPTO'11), Aug. 2011.
[11] M. Hadavi, E. Damiani, R. Jalili, S. Cimato, and Z. Ganjei, "AS5: ASecure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing," Proc. Fifth Int'l Workshop Autonomous andSpontaneous Security, Sept. 2013.
[12] "PostgresPlus Cloud Database," EnterpriseDB, http://enterprisedb.com/cloud-database, Apr. 2013.
[13] M. Armbrust et al., "A View of Cloud Computing," Comm. of theACM, vol. 53, no. 4, pp. 50-58, 2010.

BIOGRAPHIES:

TirumalaRaoGurubelli is student in M.Tech(CSE) in Sarada Institute of Science Technology and Management,Srikakulam. He has received his M.C.AIndira Gandhi National Open University (IGNOU), Delhi. His interesting areas are Data Warehousing and Data Mining.

Mr.V.Laxmiprasad is working as aAsst.professor in Sarada Institute ofScience, Technology And Management,Srikakulam, Andhra Pradesh. He receivedhisM.Tech (CSE) from GMRIT Rajam,Srikakulam District, JNTU KakinadaAndhra Pradesh. His research areas include Computernetworks, Datawarehouse and Datamining.