International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4s, November 2018

Increasing Privacy for Private Database in Cloud Environment

S. Kirubakaran, S. Karthick, S. P. Prakash

Abstract: ***After Personal computing, main frame and client server Cloud computing is a fifth generation computing. It focuses on resource sharing and computations and is a network based environment. The data will be stored enduringly information in servers on the internet and cached momentarily on clients. It has the advantage of sinking cost by allocation of computing and resource storage. Azure, EC2 Application og Google, Aneka are the processor that utilize for its operation for effective computations. The necessary resources are utilized by user through the internet. The will be raise in confidentiality issue when provider depends on other provider for resource utilizing. As there is no limits in cloud computing the data can be physically positioned anywhere in the globe. Hence the problems regarding data authentication and privacy are in raise. The privacy can be obtained by imposing access policy or by encrypting using cryptographic tools. Without leaking the important information of the owner the safety can be made ensured by safeguarding from hackers. In this proposed work a implementation authentication and authentication based on data access module and anonymity. Programming is carry out using JAVA platform and back up management using MySQL and Advanced Encryption Standard security algorithm is apply for ensuring security framework.***

Keywords: Data Authentication, Anonymity, Encryption standard, Security.

I. INTRODUCTION

The internet based advancement and computation technology demands cloud computing. The rising network bandwidth and dependable yet optimal network connections make the user to obtain high quality service Wang et.al (2010). Cloud is a system group of storage devices to merge software and data manipulation power distributed in various locations. Manipulating at cloud provide the user for super power level to access the required data. The Cloud computing can be used in access point like Apple phones, laptop, palmtops when they need them on demand basis. Security is utmost important when the resource is utilized in the private cloud. The security is crucial when the data cloud is used privately. Similarly data confidentiality is utmost important. For example the medical information about a patient is utmost important when treating a patient during emergency. These demands forces to design and implement more secure data server for improved utilization.

Manuscript published on 30 November 2018.
***Correspondence Author(s)**
S.Kirubakaran, Assistant Professor (Level II), Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam-638401,
S.Karthick, Assistant Professor (Level II), Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam-638401
S.P.Prakash, Assistant Professor (Level II), Department of ECE, Bannari Amman Institute of Technology,Sathyamangalam-638401

There is a increase concern for flexibility in today's fast moving world. The mating of an individual data base on demand can be obtained based on previously stored data base.

The data security refers to the impossibility of data usage by third party. Without leaking the important information the data should be able to retrieve by user.For example the medical information collected by an institute from the students for future reference has to be maintained. For future information the data has to be able to retrieve without any security issues and it should not be hacked by the third party. To assurance the maximum solitude to each patient, the medical facility only sends to the research database a protected description of the patient record. The known record is removed from the database when the unknown record is stored in the cloud. When a data related to drug addict has been stored in a data base. The data should be able to access by the authorized persons of the institute.

The confidentiality of the particular patient has to be kept and it should be protected. The company producing that drug for a disease will be leaked if the data storage is theft by third party. The amount of effort put forth by the company to produce that particular drug will be at vain sudha et al (2010). The secure data storage is not only the risk of the individual but also the risk of organization which may invest huge man power and resource to discover a particular issue. Hence the secure data storage with unlimited access is at most important.

II. PROBLEM DEFINITION

Data base protection is very important and plays a critical role in environment runs using cloud computing. Since could has no limit and can be access from anywhere in the world. The security and confidentiality has to be maintained. Hence in this paper a data base protection that performs to maintain the privacy and security has been proposed. This system will perform registration, verification, classification and data encryption.

III. RELATED WORK

Privacy is very important in cloud computing and a critical parameter in cloud computing environment. Garfinkel (2010) talk about how thin client and monolithic server model is realized by Google chrome OS. The privacy anxiety that the resulting data blend and data loss of infrastructural control bring to consumers Stone et al (2010). The major challenge of cloud server adaptation is privacy

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

and security. The reliable access of cloud is proposed by the providers for efficient use of cloud environment. Chow et al (2009) differentiated the cloud aces in to three types namely Information- centric, Trusted computing and privacy preserving Yao (1982). The access control policies are used to tag the data in information centric Pearson (2009).

The cryptographic protocols are selected for specific cloud applications. Chow et al (2009) proposed protocols based on cryptography for privacy-protection. Private information retrieval allows accessing the database without erudition of quires submitted by client Sion et al (2007). The owner for a set can search date by using predefined keywords by using searchable encryption without using the additional information Rivest et al (1978). Homomorphic encryption is apprehend by gentry in 2009 Gentry et al (2009) which allows computation over the data that are encrypted. In cloud environment can use server to store data without decryption the server can access the data Micciancio (2010). The server computes in high privacy way under the protection.

The special case for security is proposed by secure multiparty computation (SMC) Goldreich (2005) which pay way to manipulate the random function over private inputs. It understands, as an interactive protocol, the perfect functionality provided by a dependence party (or piece of hardware). In its universal form, however, SMC need players to be online and appropriate. Shen et al (2009) proposed the issues related to security must be included in Service Level Agreement. It describes the relationship between recipient and service provider. It explains the service definition, problem and functionality management, disaster and security recovery and the methods to standardize secure multiparty computation. It further deals with the proper termination of server. Shi et al (2007) explains the problems related to cloud computing and the various thread based on different situations. The application area defines the importance of the threat. These works gave the guidelines for service providers to make sure that privacy of the client is not affected.

IV. REQUIREMENTS SPECIFICATION

A. The requirement for Hardware

The least requirement that the system should posses has:

1. Dual core processor
2. 1GB random access memory
3. 256 GB Hard disk

B. The requirement for Software

The systems which execute the program should have:

1. Supporting Operating System: LINUX, Windows XP, VISTA
2. Java
3 SQL

C. The requirement for Network Support

The proposed project can be utilized to run on local area network and wireless communication. Which supports the network architectures like

1. Local Area Network (using network cables)
2. Wireless Network (Wi-Fi)

V. IMPLEMENTATION

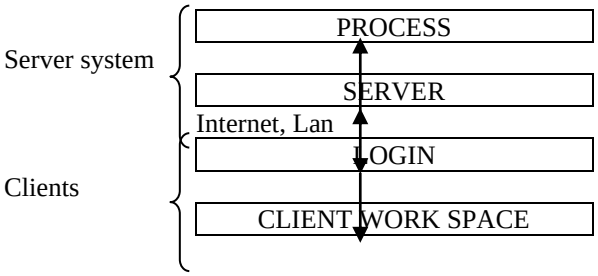

Fig. 1 Design frame work

A. Module 1: Registration module

The main parts of the proposed server can be classified in two server and client. Registration module used to create the new client of our communication purpose. This process is to create the username and password will give user interest. If once connection establish the server to client server will transfer the four digit secret key in client machine. That key will be used future reference and future process of event is used. Client is entering the wrong secret key means final operation is needed not view the client system.

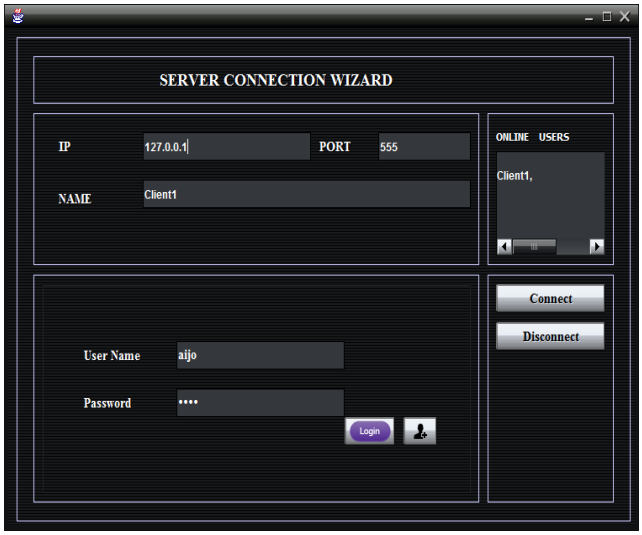

Fig.2 Client-Server Interaction

B. Module 2: Authentication of client

This module is used for security purpose. Only the authenticate person can make all the operation.

Only authorized user for using this software. Authorized users only communicate to the server. Authentication module checks user name and password server side

The client logging to server can be classified in to

1. Fresh Users
2. Existing Users

Fresh Users will have the registration form, password and username which can be added by server side to the data base.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

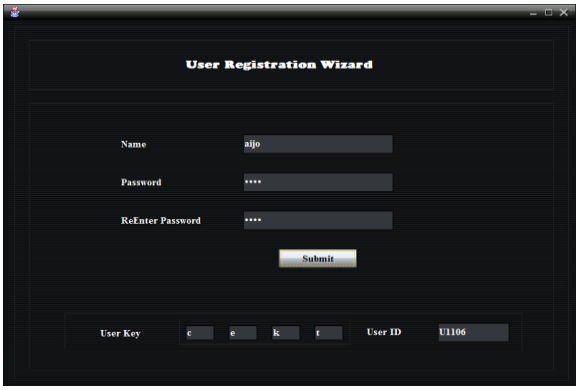

Fig.3 New user Registration form

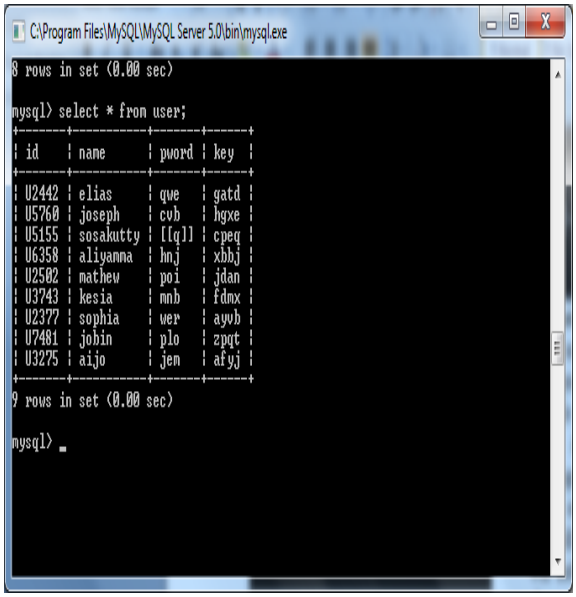

Fig.4.Data base in the server side

Existing users can provide the username and password to check their identity. In server side the username password will be stored.

C. Module 3: Classification module

Using the anonymity model the generalization of user data base is done. Over the attribute set the table T=t_1, t_2,..... t_n was considered for evaluation the set A. By masking the values of selected attributes the identical tuples are formed. According to Value Generation Hierarchies the initial values are replaced with new values.

AREA	POSITION	SALARY
Mining the data	Assistant Professor	95,000
interruption discovery	Associate Professor	80,000
Handheld Systems	Research Scholar	15,000
inquiry dispensation	Associate Professor	110,000
Digital Forensics	Assistant Professor	800,000

Table 1: Initial Data Set

Each of the given parameters can be assumed to be mapped with general value. The primary step is to replace specific value with general value based on k-anonymity protocols. Classification module classifies the user data on the user selected data set. Data set values are based on the user selected tree structure data values.

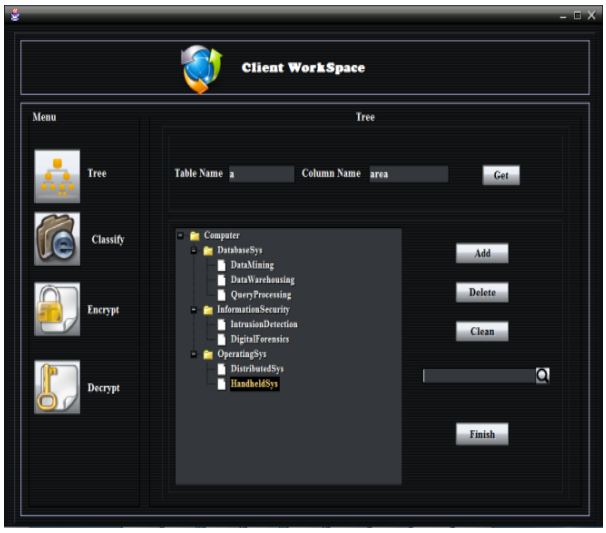

Fig.5 Value Generation Hierarchies of area

D. Module :4 Data Access Module

Data access module is used to store the encrypted data in server machine. This is module process the cryptography operation using AES cryptography algorithm. All cryptography operations is proceed is valid client only .Client give the secret key this key will be validate to server machine .client will authenticate the entry level client will choose the any process.

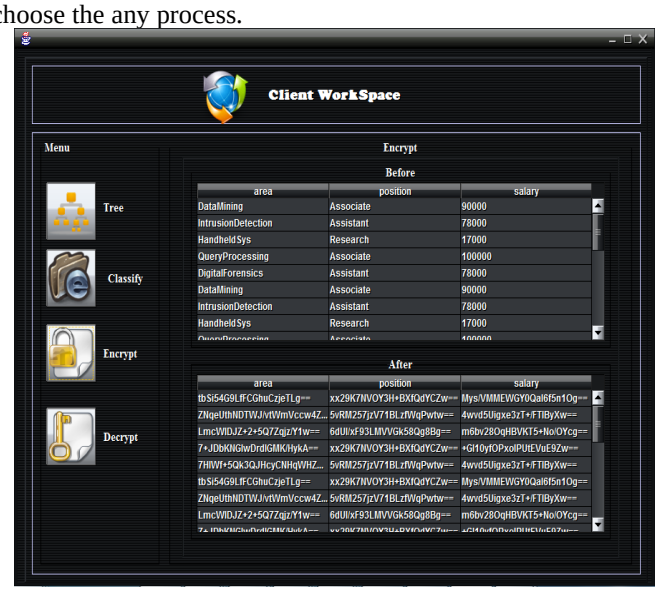

Fig.6 Encryption of dataset

Using the AES algorithm, the client encoded the data when the keys are interchanged. The system metric – encryption standard AES is used in cryptography. The block size is 128 bit size is used by ciphers with various key sizes of 128, 192 and 256 bits, respectively. The AES ciphers is used extensively worldwide which has been analyzed for its optimum performance.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The AES cipher is precise as a number of reiterations of transformation rounds that translate the input plaintext into the ultimate output of cipher text. Each round consists of various handing out steps, including one that depends on the encryption key. A set of reverse rounds are applied to change cipher text back into the original plaintext using the similar encryption key.

VI. CONCLUSION

The security and distribution of data play a crucial role in today's world. There is a higher risk for the privacy of the individual humans due to the increased attacks on their data storage when they used the public storing resource like cloud computing. A confront in today's globally network society is to allow the genuine use and distribution of information while at the same time pledge appropriate protection of the solitude of the individuals to whom information refers. The confidentiality of the personal information has to be protected by private cloud computing techniques. The issues tend to increase exponentially as the quantity of data storage increases. This proposed work demonstrates the model for data storage in cloud computing. This work in future will include more complete examination of resist third party attacks and finding where the data is stored in cloud.

REFERENCES

1. Garfinkel SL, "A less personal computer Technology Review"', May 2010.
2. Stone, B. & Vance, A, "Companies slowly join cloud computing"'. New York Times, 2010.
3. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J, "Controlling data in the cloud: outsourcing computation without outsourcing control", In Proceedings of the 2009 ACM workshop on Cloud computing security.
4. Shi, E., Bethencourt, J., Chan, T.H., Song, D. & Perrig, A., "Multi-dimensional range query over encrypted data"' In IEEE Symposium on Security and Privacy, 2007.
5. Sion, R. & Carbunar, B' "On the computational practicality of private information retrieval", In Proceedings of the Networkand Distributed Systems Security Symposium 2007.
6. Rivest, R.L., Adleman, L. & Dertouzos, M.L., "On data banks and privacy homomorphisms", Foundations of secure computation 1978..
7. Yao, A.C, "Protocols for secure computations"' In IEEE 23rd Annual Symposium on Foundations of Computer Science.
8. Micciancio, D, "A first glimpse of cryptography's Holy Grail"' Communications of the ACM, 2010.
9. Shen, E., Shi, E. & Waters, B, "Predicate privacy in encryption systems"' In Theory of Cryptography Conference 2009.
10. Gentry, C. & Boneh, D, "A fully homomorphic encryption scheme"' Stanford University 2009.
11. Goldreich, O, "Foundations of cryptography–A prime"'. Foundations and Trends in Theoretical Computer Science, 2005.
12. Sudha, M., Rao, D.B.R.K. & Monica, M, "A comprehensive approach to ensure secure data communication in cloud environment"' International Journal of Computer Applications 2010.
13. Pearson, S, "Taking account of privacy when designing cloud computing services", In Software Engineering Challenges of Cloud Computing, 2009.
14. Wang, J. & Le, J, "Based on private matching and min-attribute generalization for privacy preserving in cloud computing", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)