ISSN 2349-0292
Impact Factor 2.675

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

SECURE DATA SHARING IN CLOUD ENVIRONMENT USING CRYPTOGRAPHY

Prajwal Gowda K*, Dr. B R Prasad Babu, Mrs. Jagadevi Bakka
* M. Tech Student Dept. of CSE, R&D Centre EPCET, Bangalore
Prof. & Head Dept. of CSE EPCET, Bangalore
Associate Professor Dept. of CSE EPCET, Bangalore

ABSTRACT

Cloud computing [i] architecture provides the services for client's on-demand. It made users not to hold on any hardware requirements and complexities for maintenance. The widespread problem associated with cloud computing is data privacy. Existing system has attribute based encryption (ABE) which assigns keys for each registered clients, but the computational cost is very high and the other model is tree based key management that is designed for secure and flexible key management. In this model there is leakage for key generation and distribution. So we propose a system which uses quantum key distribute on and advance encryption standard for the users to provide confidentiality by hiding all the useful information while transferring data.

KEYWORDS: Cloud computing, Security in cloud, Quantum key distribution, Cryptography, File permission.

INTRODUCTION

Cloud computing [i, ii] is a type of internet based computing which provides the resources and the data to the computers when needed. The sharing of computing resources rather than sharing with the known servers and storage devices, it can be stored in unknown and secured devices using cloud computing. The cloud computing is categorized into parallel computing, cluster computing, distributed computing. All these patterns is categorized based their usage patterns. Cloud computing provides 3 service models which involves,

1) Software as a service (SAAS): The client can use the required software by paying small amount to service provider rather than buying them, it provides the organization to access business functionality at an affordable price that is less than licensed application, since software as a service payment is based on monthly fees.
2) Platform as a service (PAAS): Platform as a service does not completely change the business infrastructure instead a business depends on PAAS providers for key services, such as java development or application hosting. It transfers the application over the internet, cloud provider provides hardware and software tools to its users as a service.
3) Infrastructure as a service (IAAS): It provides access to computing resources in a virtual environment across a public connection. It provides online services and the details of the infrastructure which includes physical computing resources, location, partitioning of the data, scaling, security, backup etc

There are various types of security and privacy attacks in cloud computing. Some of the common types of attacks are,

1) XML signature wrapping attack: In this attack the organizational rights of the cloud user can be created, omitted, and also the images can be altered.
2) Cross site scripting attack: In this type of attack attackers will add a fragment of code into the web application to take over the mechanism of access control.
3) Flooding problems: when the harmful user sends any request to the cloud, the server gets overloaded by creating unwanted data requests in the cloud. This is done in order to extend the amount of work of cloud servers by using the huge amount of resources.
4) Denial of service: In this type of attack the harmful code is added into the browser so that it opens many windows. This prevents user access to servers.
5) Data stealing problem: here the user account details will be stolen using some techniques, so in order to prevent such type of attacks, additional values should be added during authentication. This value will be given to the right user by sending a message and thus moderate the issue of data confidentiality.

The shared data will be secured using cryptographic security mechanism and are followed in many cloud environments. Cryptography is a technique which provides security for data communication when transmitted between two parties. It analysis different protocols that avoids public from reading the personal messages. It provides different security aspects which includes confidentiality, integrity, authentication, and non-repudiation for data. In order to prevent the unauthorized access to sensitive information, cryptography uses protocols, algorithms and some strategies to securely transfer the data and it also verifies each and every component in a communication. Types of cryptography includes

1. secrete key cryptography

2. public key cryptography
3. hash functions

The main concern in cloud is data security, so the cryptographic service providers provides an individual security, attribute based encryption which is used in cloud environment and social network that permits the clients to involve in two or more groups , where the key is computed for the clients by using logical expressions.

The main disadvantage here is computational cost and rekeying. Clients are grouped with respect to their roles in which the clients can access a selected type of data only. It is also possible for two groups to view the same data. We overcome the issues of data security in cloud.

PROPOSED SYSTEM

In this paper we propose for the multiple entity key management and encryption is required, in this we come across the issue of data security while transferring data to cloud. a quantum key will be generated for the clients and to the groups by the cryptographic service provider(CSP). The user authentication is provided by 8bit random number key generation that will be sent to personal mail account of the client. The administrator will provide the access for the data storage. Access for the groups is based on the type of the file shared by the user to the cloud database.

After selecting the file that has to be transferred, then the user will be provided with the quantum key and the IP address to store the data. After file is successfully transferred to the database, it gets decrypted only when user access the file.

ALGORITHM:

Step1: client login to cloud
Step2: client selects a file (F)
    If F=1 then move to step 3
    Else
    F is discarded
Step3: client request CSP for cryptographic service
Step4: N=file size (F), is used as input to generate quantum keys
Step5: file size is split into 2 values (V1 and V2)
Step6: V1 and V2 are computed to produce quantum key
    K1=V1 mod [number of digits in N]
    K2=V2 mod [number of digits in N]
Step7: k1 and k2 are used to encrypt the file (F)
Step8: the encrypted file is sent and stored in cloud.

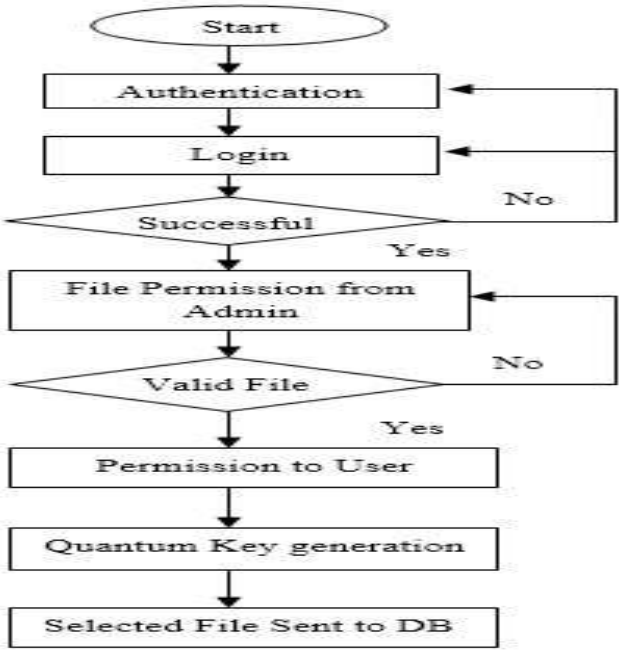

Figure 1: Flow Chart of the Proposed System

ISSN 2349-0292
Impact Factor 2.675

Figure 2: Log-In Form

The user registers their details and for authentication purpose. The user then have to login with the help of login-form the user enters the required credentials such as user name and password for a successful login

Figure 3: Provider Form

Figure 3 represents the provider form the user can select the file, if it is a valid file then the user can proceed further taking the file as an input and quantum key will be generated. By using this quantum key distribution the file will be encrypted. If the file is not valid then a pop-up message appears stating "User can't share this file".

Figure 4: IP address form

Figure 4 represents the IP address form which provides the location for encrypted file to store in the cloud. The storing file can be given with the file permission that may be private, public and protected. It also provides the details of previously uploaded files

ISSN 2349-0292
Impact Factor 2.675

CONCLUSION

Cloud computing permits the consumers to use the applications without any installation process and allows the users to access the files at other systems through the internet. Data security is the main problem. To overcome from this problem, we use quantum-cryptography-as-a-service (QCAAS) which uses an quantum advanced encryption standards and provides quantum cryptographic keys to secure the file from any kind of security issues. This project involves both Cryptographic Service Provider (CSP) principles and Quantum key Distribution mechanisms.

REFERENCES

[1] Omer K. Jasim Mohammad, "securing cloud environment using new trend of cryptography", IEEE, 2015.
[2] Nelson G, Charles M, Fernando R, Marco S, Tereza C, Mats N, Makan P, "A quantitative analysis of current security concerns and solutions for cloud computing", Journal of Cloud Computing: advanced systems and applications, springer, vol.1, No. 11, 2014.
[3] Omer K Jasim, Safia Abbas, El-Sayed M El-Horbaty and Abdel-Badeeh M Salem, "A Comparative Study between Modern Encryption Algorithms based on Cloud Computing Environment", International Conference for Internet Technology and Secured Transactions, UK, December 2013.
[4] D Chen and H Zhao, "Data security and privacy protection issues in cloud computing", International Conference on Computer Science and Electronics Engineering, ICCSEE, IEEE, vol. , 2012.
[5] Rawal V, Dhamija A, Sharma S, "Revealing New Concepts in Cryptography and Clouds", International Journal of Scientific and Technology Research, vol.1, No. 7, 2012.
[6] Xing Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", Department of Computer Science and Technology Harbin, 2011.
[7] Q Zhang, L Cheng and R Boutaba,"Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications, vol., no.1, 2010.
[8] Bertino, R Ferrini, "Privacy-Preserving Digital Identify Management for Cloud Computing", IEEE Data Eng., vol. 32, no.2, 2009.
[9] R Buyya, C S Yeo, S Venugopal, J Broberg, I Brandic, "Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility", Further Generaion Computer Systems, vol.25, no.6, 2009.
[10] A.D. Kshemkalyani, M. Singhal, and Distributed Computing: Principles, Algorithms, and Systems, ISBN: 9780521189842, paperback edition, Cambridge University Press, March 2011. 756 pages. 2008.

ACKNOWLEDGEMENT

Mr. Prajwal Gowda K is M.Tech Scholar in Computer Science and Engineering at East Point Collage of Engineering and Technology, VTU. I attended and presented more than 3 papers in National and International Conferences in various collages. I had attended the Handson workshop in CSI Bangalore Chapter and also attended the Handson workshop on Big Data. My research areas are Cloud Computing and Big Data.

Mrs. Jagadevi Bakka is working as Associate Professor R & D Dept of Computer Science and Engineering at East Point Collage of Engineering and Technology. Her research area is networking. She published more than 6 papers in various International Journals.

Dr. B R Prasad Babu is working as Professor and Head, Dept of Computer Science and Engineering at East Point Collage of Engineering and Technology. His research areas are Mobile Adhoc Networks, Mobile Communication and Software Engineering. He published more than 50 papers in various International Journals. Presently he is guiding for PhD Scholars in Visvesvaraya Technological University (VTU) and Jawaharlal Nehru Technological University (JNTU) India