Advanced Data Security using Homomorphic Algorithm in Hybrid Cloud Computing

V.Ramya
Dept of computer science
SRM Institute of science and technology, Chennai

Abstract- *Cloud computing is spreading around the world, need of inter cloud communication is becoming a growing in the organizations. Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models and deployment models (private, public, hybrid, and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers. The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures. The techniques which can be used in hybrid cloud securities can be built around the encryption and decryption of data, key based security algorithms which are mainly oriented on authentication and authorization techniques as in wired and wireless networks. One such mechanism is to share the challenge text between the clouds before actual communication should start for authentication. The various works done in this area till date are oriented on other techniques of security between the two or more clouds in a hybrid cloud.*

Keywords- cloud computing, hybrid, cloud, challenge, text, security

I. INTRODUCTION

A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms. 2. A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party. This type of hybrid cloud is also referred to as hybrid IT.

II. PROBLEM IDENTIFIED

Our main objective is to preserve sender authentication, receiver authentication, message integrity and confidentiality of data in the cloud environment. Since private key cryptography can be used to provide confidentiality but in cloud it faces the problem of distributing the shared key so that only two people have it. Hence RSA can be used. So the second goal is to maximize the efficiency of public key cryptographic Algorithm RSA since its very slow due to large number of mathematical computations involved. RSA is secure till the time there does not exist the fastest prime factorization method. Elliptic curve is there but its not that fast if very large numbers are chosen for key generation by RSA.

III. SECURITY ISSUES

Cryptography technique

There are so many cryptographic Algorithms for dealing with security issues but since data is big in cloud usually in Tera Bytes and un-scattered as it could be of any type i.e. image, text, etc. one cannot provide the security in cloud computing using traditional cryptography Algorithms. Big Data has three features - Volume, variety and velocity. Volume means large amount of data is stored in data centers, variety means the data is of different type- it could be image, text etc. and velocity means the speed of data processing. In the existing work, it has been shown that RSA being the most popular and simple Algorithm could be used for secure cloud computing. It has been designed after Diffie Hellmans secure exchange of public keys protocol. This Algorithm is based on modulo arithmetic. It selects two large prime numbers and then calculate public and private keys on the basis of a mathematical formula i.e. $c = m^d \bmod n$ and $m = c^d \bmod n$ for encryption and decryption respectively. In this Algorithm, even if someone gets access to the public key; he or she cannot find out the message without the private key and the private key is present only with the person for whom the message is sent. Hence, it is secure but what if someone impersonates someone else and gets access to his messages.

a) Confidentiality

A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. Encryption is VERY widespread in today's environment and can be found in almost every major protocol in use. A very prominent example will be SSL/TLS, a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

b) Integrity

As with data confidentiality, cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as GPG to digitally sign the data.

c) Availability

Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. Almost every week you can find news about high profile websites being taken down by DDoS attacks. The primary aim of DDoS attacks is to deny users of the website access to the resources of the website. Such downtime can be very costly. Other factors that could lead to lack of availability to important information may include accidents such as power outages or natural disasters such as floods.

III. HOMOMORPHIC ENCRYPTION ALGORITHM

Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of homomorphic encryption is to allow computation on encrypted data.

Cloud computing platforms can perform difficult computations on homomorphically encrypted data without ever having access to the unencrypted data. Homomorphic encryption can also be used to securely chain together different services without exposing sensitive data.

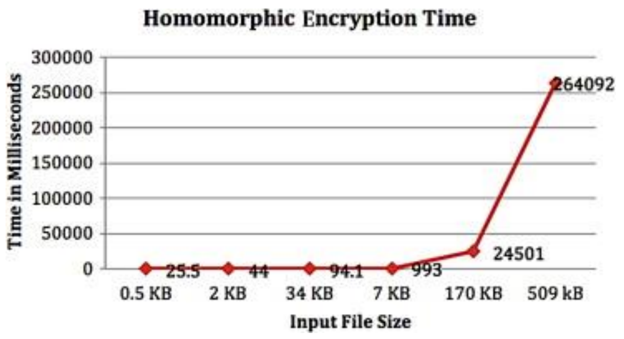
IV. SAMPLE DATA

Input is given as J=14883982794894487223, K=43321 and number to be encrypted N=9 Then D and F are calculated as
D=70677186543966147614195862042065680704217811307
170938823680817972460078770747 and
F=730390473299616118774746223206442922044393268447
47783070676806904287578243639 Consider four bit number K' = 12 then compute
P0=10519580285119403059293206075655334278355741466
4099137669178122750463891978223732486512473
7665581 and
P1=10871119238146327664815812416970040873377501996
7891779423494587651257282914457503860391386
7044349 Perform Encryption and get
C=35153895302692460552260634131470659502176053037
92641754316464900793390936233771373878912937 87689.
Decryption is performed and get back plain text N=9

V. IMPLEMENTATION

The user can connect to the AWS DynamoDB service through the Eclipse IDE for Java EE Developers. This allows the user to login based on his credentials and then the user can perform operations on their data based on requirements. Once user is done with all the tasks, it can opt to exit the system. The following are the steps performed for the implementation Step

1: Create a DynamoDB instance on AWS
Step 2: Create Database Tables with proper schema
Step 3: Get the credentials from AWS and perform access controls
Step 4: Install Eclipse Kepler version and Java SDK on it After the installation of AWS SDK on Eclipse framework the user is available with all the needed packages.
Step 5: Follow the steps given in23AWS SDK.



VI. CONCLUSION

Cloud Computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges are still existing in this technology. Security is the most challenging issue in this technology. In this paper we have discussed various encryption algorithms to overcome this security issue, deals with advantages and disadvantages of these algorithms. Here we conclude that homomorphic algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. The ability of homomorphic algorithm to perform operations on encrypted data enables high security than other algorithms such as RSA, DES, AES. Future work is to implement hardware or software technique with homomorphic algorithm to provide protection on cloud from any type of security attack.

REFERENCES

[1] Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360- Degree Compared CoRR. abs/0901.0131.

[2] Satyakam Rahul, Sharda, “Cloud Computing: Advantages and Security Challenges” International Journal of Information and Computation Technology, vol. 03, 2013

[3] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud- computing-security-risks-853.

[4] Anca apostu, Florina puican, Geanina ularu, George suciu, Gyorgy todoran, “Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud”, Recent Advances in Applied Computer Science and Digital Services

[5] Srinivasa rao v, Nageswara rao n k, E Kusuma kumari, “Cloud Computing: An Overview”, Journal of Theoretical and Applied Information Technology.

[6] Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012

[7] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009

[8] Samyak Shah, Yash Shah, Janika Kotak, “Somewhat Homomorphic Encryption Technique with its Key Management Protocol”, Dec 14 Volume 2 Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 4180 – 4183

[9] Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.

[10] Gentry, Craig. "Computing arbitrary functions of encrypted data." Communications of the ACM 53.3 (2010): 97-105.