INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

IMPROVED SECURITY MEASURES FOR DATA IN KEY EXCHANGES IN CLOUD ENVIRONMENT

Merlin Shirly T[1], Margret Johnson[2]

[1]PG Full Time Student, Computer Science Department, Karunya University, Coimbatore
[2]Assistant Professor, Computer Science Department, Karunya University, Coimbatore
[1]merlinshirly@gmail.com, [2]margret_cse@karunya.edu

Abstract

The Cloud Environment provides the distributed facilities to the user that reduce the cost of purchasing their own Computing Environment. The Vast storage is needed for storing the Big data for scheduling in Hybrid Environment. The data security is the main concern in Cloud Environment. So, the data are encrypted before storing in cloud. The asymmetric Encryption algorithm provides more security in insecure medium. Since, the private key of the RSA algorithm is known only to the authorized user. Here, the controller after receiving the data from the user starts the key exchange in order to authenticate the Server Instances. The key exchange is done using Diffie-Hellman Key Exchange Algorithm. The digital Signature Algorithms are also used along with the Diffie-Hellman Key Exchange Algorithm in order to prevent man-in-middle attack. After the authentication of the Server Instances by the Controller, the Controller split the big data and Encrypt the data using public key of RSA algorithm. Then, the controller splits data and sends it to the Server Instances for Computation.

Keywords*:* Cloud Environment, Hybrid Environment, Authentication.

1. Introduction

Cloud Computing is a new technology that uses the Central Servers in order to maintain data. The data over the cloud storage needs encryption. The encryption of the data uses RSA algorithm. The algorithm features are as Secrecy, Authentication, Non-Repudiation, Integration and Privacy [2]. The Cloud storage is the storage of data in the cloud. The advantages of cloud storage are Cloud storage greater accessibility, reliability, strong protection for data back, archival and disaster recovery [1].The type of cloud storages are Personal Cloud Storage, Public Cloud Storage, Private Cloud Storage and Hybrid Cloud Storage.

The Public-key cryptography is referred to the algorithm that has two keys for encryption and decryption. The Keys are mathematically linked together even though the keys are different. The public key is known to everyone but the private key cannot be calculated from the public key. In RSA Encryption algorithm, the public key is known to everyone so anyone can encrypt the data. But, the decryption key is known only to the authorized individual. So, the authorized receiver can only decrypt the data.

2. Proposed Method

The proposed approach for Key Exchange uses Diffie-Hellman Key Exchange along with the authentication step for each of the controller and the Server Instances. The Encryption of data using RSA algorithm provides strong security for data over insecure medium. Already the Digital Signature is used along with the Diffie-Hellman approach in order to authenticate each other [3]. After the authentication of each Servers and the Controller, the user data is split and encrypted and sent to the Server Instances for computation.

2.1 Architecture

The Architecture diagram of the Improved Security Measure of Data in Key Exchange scheme is shown below. The user gives the data to the Cloud Controller for computation. The controller starts the key exchange in order to authenticate the cloud server instances. After the authentication of Server by the Controller the data are encrypted using RSA encryption algorithm. The encrypted data are split and sent to the Server Instances. The Server Instances decrypts the split data and computes the data. After computation the data are encrypted and sent back to the Controller.

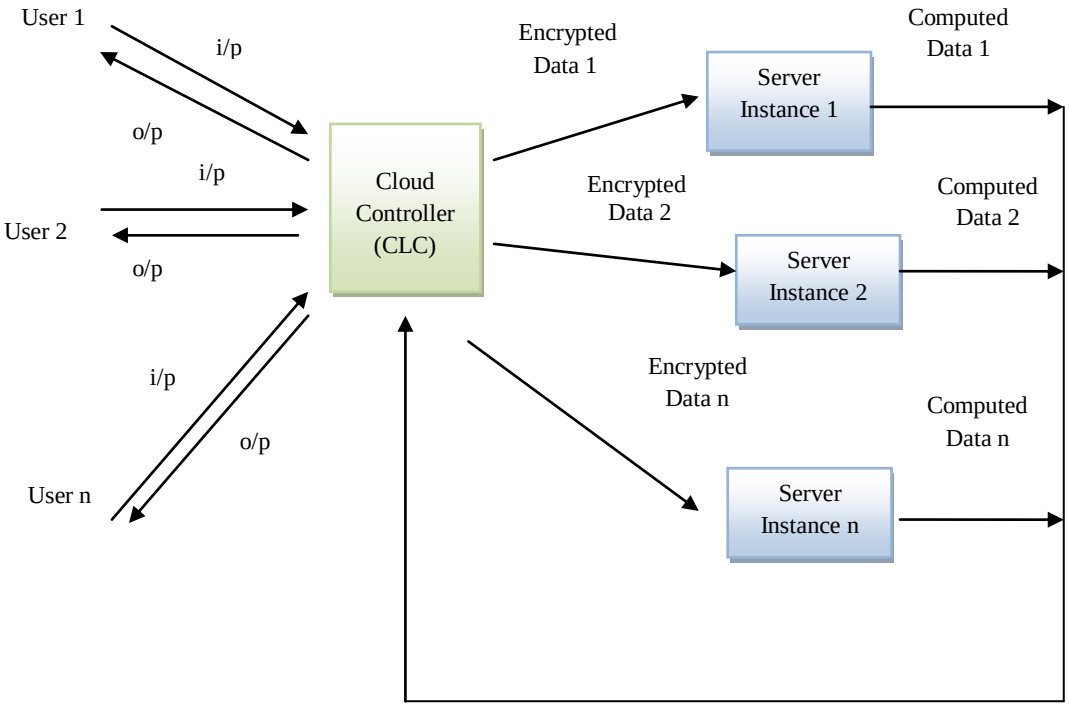
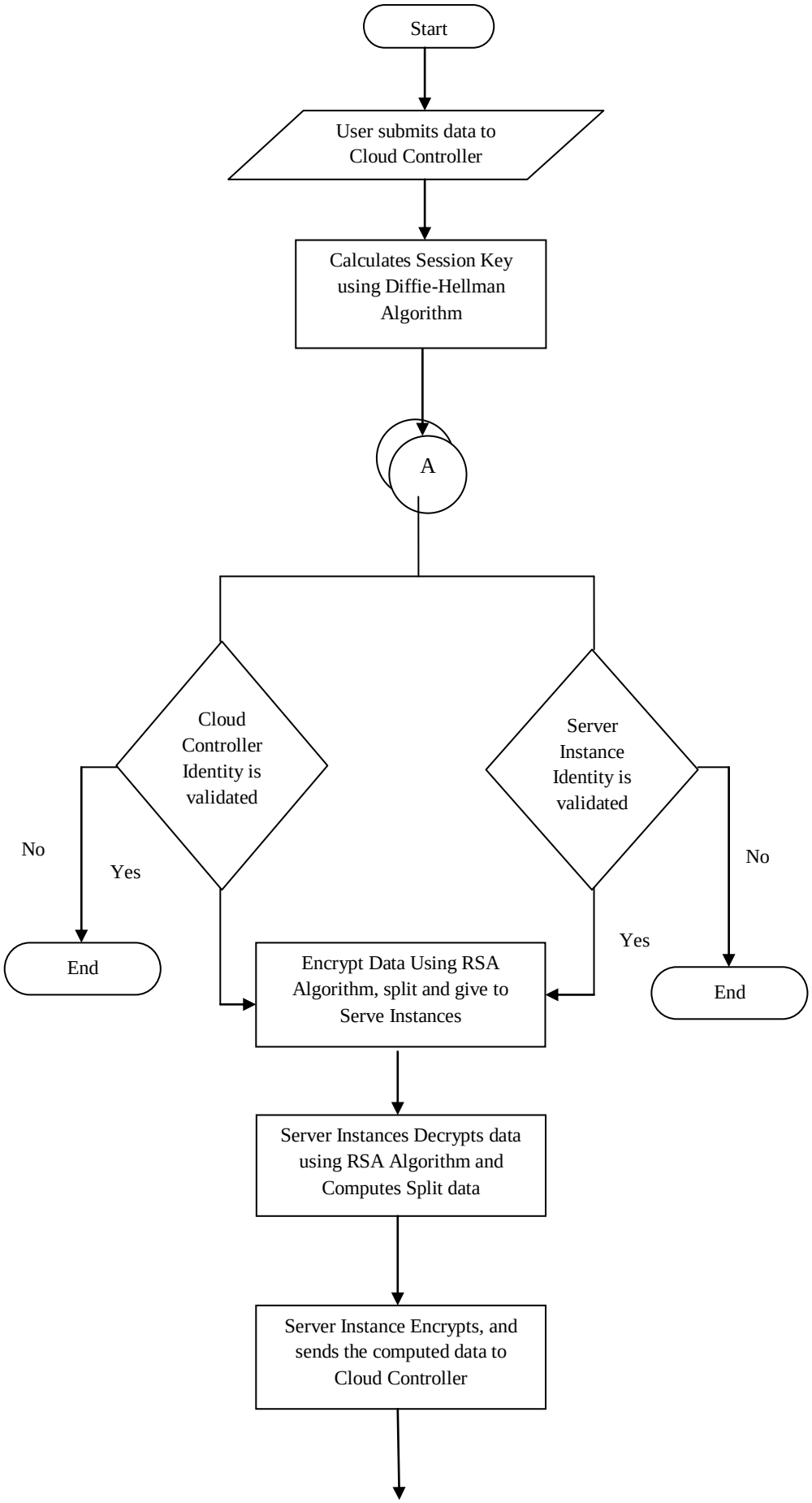


Figure 1: Architecture Diagram of Improved Security Measure in Key Exchange Scheme

2.2 Flow Chart

The user submits data to the Cloud Controller and the controller validates the Server Instances by exchanging the Session key. The Session Key is exchanged between the Controller and the Server Instances by using the Diffie-Hellman Key Exchange Algorithm. After the verification of the Server Instances and the Controller identity, the data are encrypted using RSA Algorithm. Then, the encrypted data are split and send to the Server Instances. The Server Instances decrypt the split data using the RSA Algorithm. The Decrypted split data are computed in the Server Instances. The computed data are Encrypted and sent to the Controller. The Controller decrypts and assembles the data from the Server Instances


Start
User submits data to Cloud Controller
Calculates Session Key using Diffie-Hellman Algorithm
A
Cloud Controller Identity is validated
Server Instance Identity is validated
No
Yes
No
Yes
End
Encrypt Data Using RSA Algorithm, split and give to Serve Instances
End
Server Instances Decrypts data using RSA Algorithm and Computes Split data
Server Instance Encrypts, and sends the computed data to Cloud Controller

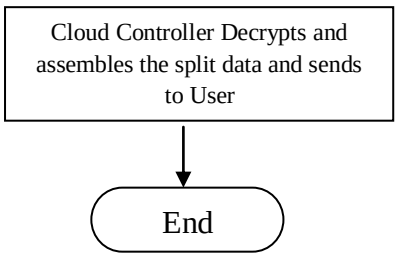


Figure 2: Flow Chart of Improved Security Measures in Key Exchange Approach

2.3 Methodology

The main steps involved in Improved Security Measures in Key Exchange Scheme are Task Submission and System Setup, Controller Key Transformation and Server Instance Key Transformation. These 3 modules are given below.

2.3.1 Task Submission and System Setup

In task submission module, a user task is submitted by the user. The user task contains larger data and it is submitted to the Controller. For task execution process, the system setup is processed. For secure data execution and transformation, the system chooses a large prime integer p to form a Diffie–Hellman group, and a generator g of group. The prime number that is chosen should be a Sophie Germain prime where (p − 1)/2 is also prime, so that the group Z∗ p maximizes its resilient against square root attack.

2.3.2 Controller Key Transformation

The Cloud Controller needs to distribute the user tasks on the computing infrastructure. The Cloud Controller picks a secret value x<p, then computes public keying material g^x in Z^*_p, and sends the message to server instances. The Cloud Controller picks a secret value x. The secret value x should be less than the prime integer chosen by System Setup. By using that secret value x, CLC computes its public keying material g^x in Z^*_p, and broadcasts the following message to the domain of server instances S which contains n instances $S_1, S_2, \ldots\ldots S_n$. The Secret Key is calculated by using Diffie-Hellman Key Exchange Algorithm. The Cloud Controller calculates the Controller's Public Value X_C. The Controller sends the Public Value, X_C to the Server Instances. After receiving the Controller's Public Key X_C, the Server Instance calculates the Session Key.

2.3.3 Server **Instance** *Key Transformation*

The Server Instance calculates the Public Key, X_S and sends the Server Instance's Public Key to the Cloud Controller. After receiving the Controller's Public Key, the Server Instance calculates the Session Key. Thus, the Session Keys are calculated at the Cloud Controller Side as well as in the Server Instances by using Diffie-Hellman Key Exchange Algorithm.

2.3.4 Signature Generation

The Cloud Controller loads the encrypted data into Hadoop Distributed File System. The RSA Algorithm is used for Encryption and Decryption of data. The Hadoop Distributed File System has five nodes namely Data Node, Name Node, Secondary Name Node, Job Tracker and Task Tracker. These nodes serve as the Server Instances. The Cloud Controller split the encrypted data and sends it to the nodes. The Cloud Controller generates signature using its secret key for n messages to be sent. The Cloud Controller sends the signature and task details for successful task execution and task transformation. Signature generation will be done in windows using java language and it will be transformed to Ubuntu platform through eclipse IDE using MapReduce perspective. Hadoop will be configured and opened as a virtual machine in VMware workstation which enables a system to run more than one operating system. Each server instance follows the same procedure to send back the executed task to Cloud Controller.

2.4 Use of Diffie-Hellman Key Exchange Algorithm

2.4.1 Session Key Calculation at the Controller

The Controller chooses a larger Prime number P, a generator g, the primitive root of the prime number P. Choose a secret Value X_C, the private key. Calculate Y_C, the public key. $Y_C = (g)^{X}_{C}$ mod p Send Y_C, the Controller's public key to the Server side Receive Y_S, the Server's public key from the Server side. Calculate S, the Controller's Session Key. $S = (Y_S)^{X}_{C}$ mod p.

2.4.2 Session Key Calculation at the Server Instance

The Server Instance choose the large prime number p, a generator g, the primitive root of the prime number p. Select secret value X_S, the private key Calculate Y_S, the public key. $Y_S = (g)^{X}_{S}$ mod p. Send Y_S, the Server's public key to the Controller side. Receive Y_C, the Controller's public key from the Controller side. Calculate S, the Server's Session Key. $S = (Y_C)^{X}_{S}$ mod p.

3 Results and Analysis

The Improved Security Measures for Data in Key Exchange over Cloud Environment provides high security in terms of Big data Encryption. The Key Size of RSA Algorithm is up to 4096 bits. Thus security increases as the Key size increases. This approach provides perfect forward Secrecy and also reduces the computation load due to the decreased number of exponential calculations in the Secret key calculation rounds. In Big data, Security is the main concern and it is achieved using the Asymmetric algorithm such as RSA.

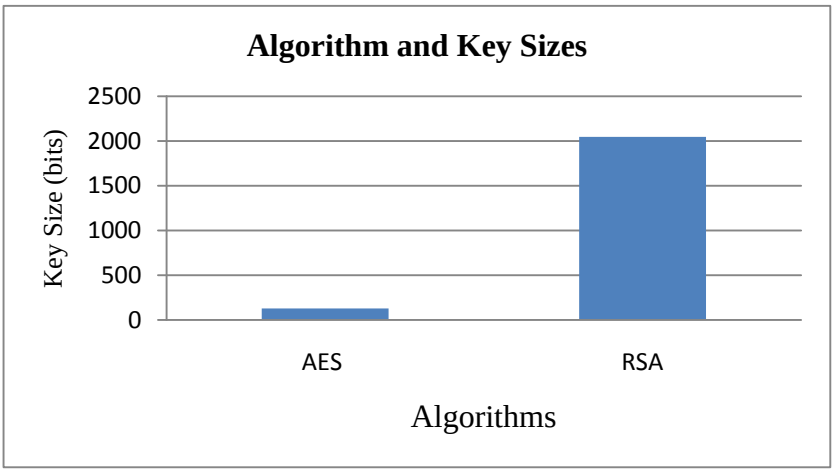


Figure 3: AES and RSA with 2048 bit Key Size

The Secret key need not to be sent in the insecure medium since it is calculated by the Authorized individual. In fact the secret key cannot be generated from the public key that is broadcasted. The RSA algorithm Key Size can be from 2048 bit to 4096 bit

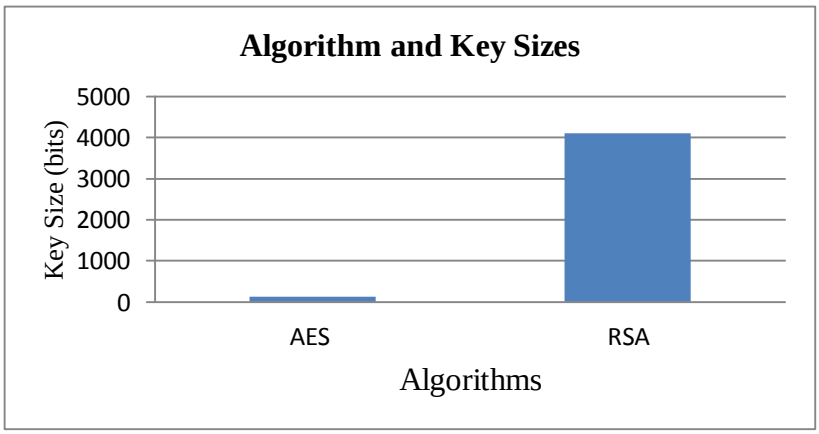


Figure 4: AES and RSA with 4096 bit Key Size

4. Conclusion

In Improved Security Measures for Data in Key-Exchange Approach the jobs are efficiently executed in parallel processing environment called Hadoop and the this scheme aims at efficient security – aware scheduling of data intensive applications in hybrid computing environment such as cloud computing. The Asymmetric Encryption Algorithm provided high security with the increased Key size used for Encryption and Decryption because security is the main concern in Cloud Storage Environment.

5. Reference

[1] Cloud storage. Available: http://www.webopedia.com/TERM/C/cloud_storage.html, accessed on 13 March, 2014

[2] RSA Algorithm. Available: http://en.kryptotel.net/rsa.html, accessed on 13 March, 2014

[3] L. Harn, "Digital signature for Diffie-Hellman public keys without using a one-way function", Electronic Letters 33(2), 1997.

[4] Chang Liu, Xugun Zhanh, Chi Yang, Jinjun Chen, " CCBKE – Session Key Negotiation for Fast and Secure Scheduling of Scientific Applications, Future Generation Computer Systems (29) 2013.