International Journal for Rapid Research in Engineering Technology & Applied Science
Vol VIII Issue VI June. 2022
ISSN Online: (2455-4723)

Strong Authentication Policy for Cloud Computing Environment Using Modified Kerberos Authentication Protocol

M.tech. Scholar Niklesh Jadam, Assistant Professor & Head Mohit Jain
Computer science , BM College of Technology Indore (M.P) Country
nikleshjadam@gmail.com, bmctmohitcs@gmail.com***

ABSTRACT

Cloud computing is one of the leading phenomenal topic of nowadays. It raises the working nature of business. Cloud Computing is a very popular term in the field on computer science as the name describes, it completely means computation of data in a large environment. Anotherward, Security is one of the crucial and important factors in cloud computing environment. Here, possibility of improvement has been observed in dimension of security and enhanced authentication protocol has been explored. In this work we have developed a strong cloud environment using Kerberos authentication protocol. The problem and algorithm proposed is based on security of data in cloud environment. Where, modified algorithm of Kerberos is used. Along with it RSA and ECC is also used this approach is used for encryption and decryption. Kerberos algorithm is applied when client wants to access the data.

Keywords: *Cloud computing; Security; Kerberos protocol; RSA; ECC*

1. INTRODUCTION

Cloud computing is widely used in many organizations and also adapted to access different services provided by cloud. It has a capability of storing, sharing, accessing, processing and networking. Customers can use cloud to deploy, develop, execute and run their software with providing necessary resources as required. This environment of cloud computing creates storing and sharing of resources whose extension cannot be defined.

A. Service models of cloud computing

Cloud computing provides various services in the form of service models and these models are classified into three categories:

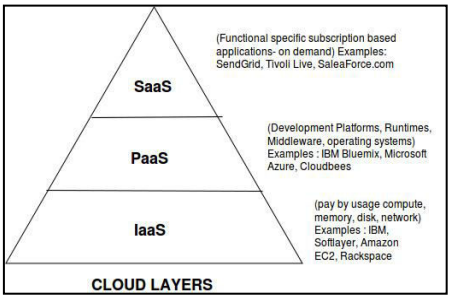

Figure 1: Services of cloud

1. Software-as-a-Service: Software-as-a-service is defined as a service model in which the vendors provide application and available those applications for user over Internet.

2. Platform-as-a-Service: The service provided by this service model can be used to manage, develop, execute and run the application on the provided platform. A platform is provided to user on rent, which he can perform computation, processing and operation.

3. Infrastructure-as-a-Service: In infrastructure-as-a-service a virtual infrastructure is provided to customer where he can use any virtual machine as required and have to pay-per-use. A virtual space with network is provided to user, which can be managed by platform as a service.

B. Types of Cloud Computing:

On the basis of models cloud is categorized into four types:

1. Public Cloud: In public cloud resources can be accessed inside or outside. Anyone at anytime can access the resources.

2. Private Cloud: In private cloud if any organization owned a service then that owned service is accessed by that specific organization.

3. Hybrid Cloud: The combination of public and private cloud is called hybrid cloud. It is done so as to get best service.

4. Community Cloud: Any organization can owned the services and made them common to use for particular community.

2. RELATED WORK

Vishwanath et al. In[1] described that to increase the security of data RSA algorithm is implemented and the uploaded data on cloud is stored temporarily. To store that data permanently RSA algorithm is used, which provide security to data and control data loss.

Uma Somani et al. In[2] proposed about data security authentication using digital signature. It can be detected that user is authenticated or not using digital signature.

Nicholas et al. In[3] describes about virtualization, software and hardware also supports virtualization. Virtual hardware is supported in cloud computing. Many operating system, infrastructure are managed by cloud platform. Dynamic and distribution is also a feature of cloud after virtualization.

Ya-Qin Zhang et al. In[4] described about client side cloud computing which is the future of cloud computing. Where, client can access any services and resources of cloud and deploy to form dynamic. Dynamic refers to the transformation into physical resource. Client play a very essential role in cloud computing.

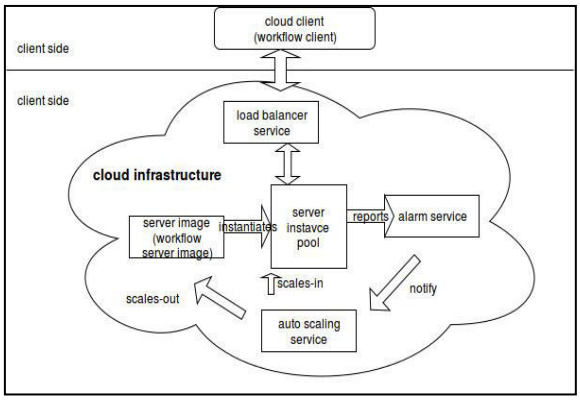

Figure 2: Cloud Client

Chow et al. In[5] proposed about the secure system for storage in cloud. In this secure storage system cryptography is used for encryption and encryption is done to control data loss and integrity of data.

Fatemi Moghaddam et al. In[6] using some tool and techniques described about authentication schema. This schema of client based authentication is to identify the identity of user.

Zarandioon et al. In[7] describes about key to cloud which is based on encryption and signature. It is user-centric, manages and controls the access of data. Virtually manages the services of cloud.

A. Abuhussein et al. In[8] focuses on security issue which is the major concern. A example of dropbox is taken which is the tremendous security lapse of that time.

J. Varia et al. In[9] proposed about service platform, which is the open source platform. Amazon which is the vast resource storing provider shares huge resources in free of cost and also provide other vendors to get services in effective way.

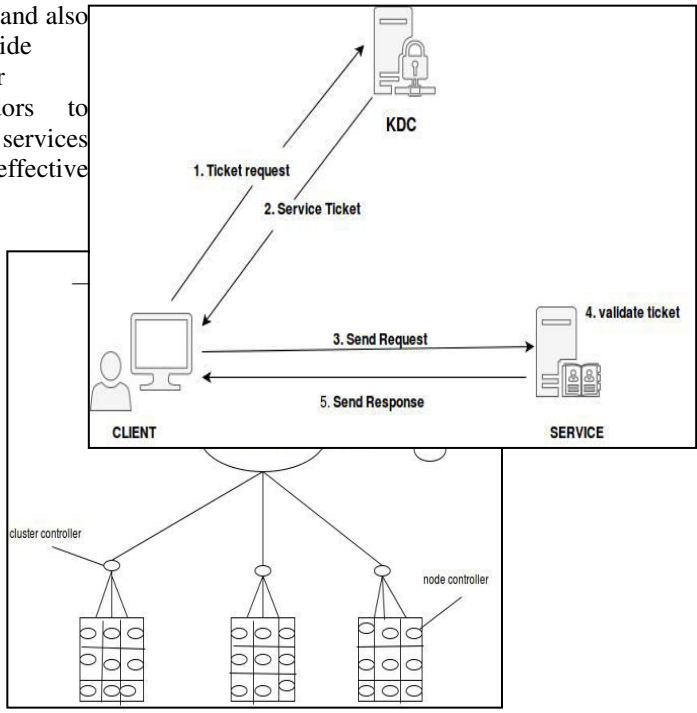

Figure 3: Amazons open source cloud vendor

G. Haff et al. In[10] describes that open source cloud provide its customers with best services which fits best to the specific organization. To form their own cloud it provides its user with software and hardware.

M. Miller et al. In[11] indicates about the use of Internet. Thousands of people are working and using Internet daily, in which many computer networks are interconnected to serve there customers with proper service.

J. Rhoton et al. In[12] proposed about the services of cloud. These services serve the user with database, virtual machine, application, software and infrastructure to work.

3. PROBLEM DOMAIN

With the rapid growth in cloud computing, Information Technology is also increasing. It is a large interconnected network which is widely used. Its services, platform etc are used by user. Services, platform and sharing are different thing, with all this, security is very important for storage and accessing of any data i.e. some mechanism are required which will provide security to the user and server of cloud. This feature of security is authentication, availability, confidentiality, and encryption. Authentication is an approach which ensures that request is from specific user and no interference will occur. If there is no trust relationship between sender and receiver then no third party provider is required.

If security is not provided to user then it is big risk to loss data and accessing of attackers. Many security mechanisms are applied in order to achieve trusted relationship between client and server.

The strong authentication protocol in cloud computing is achieved using Kerberos algorithm along with RSA and ECC.

RSA and ECC are used as encryption and decryption technique for security purpose; there work is based on keys. These keys are responsible for encryption and decryption, these keys are called public and private key.

Figure 4: Architecture of Kerberos protocol

The complete work observes that the algorithm used are beneficial and through it, it can be concluded that on the basis of need of cloud, better security is implemented. Kerberos is a good technique whose authentication is under KDC. Ticket granting approach is very strong in achieving security. Suggested security work in cloud is based on architecture.

4. METHODOLOGY

A very well-known security protocol used called as Kerberos authentication protocol:

Kerberos is an authentication protocol for computer networks; its work is based on tickets, which gives permission to the nodes that are communicating over the network which is not secure and proves their identity in secure manner. On the name of author Kerberos the protocol was named. Its design is like client-server model. In client-server model, the user and server both verifies their identity. This protocol protect against attacks.

Client sends the request to authentication server which authenticates client identity and forwards it to the Key Distribution Center (KDC). Authentication server sends Ticket Granting Ticket (TGT) to client in the encrypted manner and was encrypted using secret key. TGT expires after sometimes but can be renewed again at the time of login session. If client communicates with another node, he sends TGT to Ticket Granting Service (TGS), which shares the same KDC, client request for server access from TGT. Then it is verified that TGT is valid or not, if is valid then it is allow to access the service. Ticket Granting Service (TGS) send the send the ticket and encrypted session key to client. The client then sends the ticket to the client service provider with request and services provider encrypt it and send for client validation.

RSA Algorithm:

RSA algorithm is an asymmetric cryptographic algorithm used for encrypting and decrypting messages. In asymmetric there are two keys, Public key and Private key.

The public key is known to everyone and used to encrypt message. Messages which are encrypted using public key are decrypted using private key in RSA algorithm. Private key is the secret key. These keys are helpful for securing data transmission key generation.

ECC Algorithm:

ECC stands for Elliptic Curve Cryptography. ECC is a public key encryption technique based on algebraic structure. It is developed by Vector Miller and Neil Kobitz in 1985. It also works as an encryption cryptographic technique.

Equation of elliptical curve is:

$$y^2 = x^3 + ax + b$$

Flow of proposed methodology

The proposed methodology explains the flow of work using different algorithms like RSA and ECC along with Kerberos protocol. Flow implementation is defined as :

1. User login request.
2. User authentication through Kerberos.
3. If valid user then token generate through RSA.
4. Resource server verifies the token.
5. If token matched then select the file for uploading.
   (Digest the selected file using MD5 algorithm)
6. Divide the file into chunks.
7. Encrypt the file using ECC algorithm.
8. Upload the file on cloud server along with digest.
9. Download the file
   (Digest the downloaded file using MD5 algorithm)
10. Decrypt the file using ECC.
11. Match both the digested file.
12. If matched then file is downloaded.

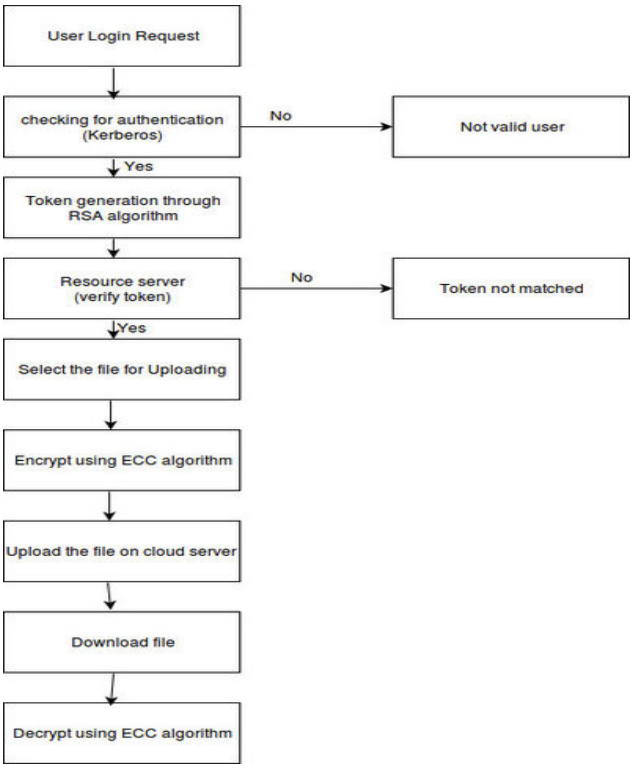

Figure 5: Flowchart of proposed work

5. IMPLEMENTATION STRATEGY

The proposed solution indicates the use of algorithm for strong authentication in cloud computing using modified Kerberos authentication protocol.

Kerberos authentication protocol is secure using various key features:

KDC: KDC is the Key Distribution Center consist of authentication server (AS) and ticket granting service (TGS).
AS: AS is the authentication server which authenticates the user identity.
TGS: TGS is the ticket granting service which sends ticket to user.

User-Client login: user enters his username and password after it security credential is generated in the form of public key, which is to be entered in place of password. Client changes the password in form of key.

Client Authentication: client sends message to authentication server (AS). The authentication server authenticates the information of client, whether it is stored in database or not. If it is available then authentication server generates key and sends encrypted session key using secret key to client. TGT is permitted to client and encrypted TGT with time validation is also sent to client. As the message is delivered to client, he decrypts the message using the secret key.

Client-Service Authorization: client request the service from TGS, TGS retrieve the message and decrypt it using secret key (using TGS secret key, decrypt the message).

Client-service Request: after receiving messages client authenticate it and sends message. Service server decrypt the ticket using secret key and retrieve the session key. Using session key the service server authenticate the client identity, if it matches then SS sends message to client to confirm his identity and serve the client. Client decrypt message using session key, if it is correct then server is trust-able and can request services from server. Server will provide the requested service to client.
RSA algorithm is used for encryption, when the client sends request to authentication server, it authenticate client and generate token. Here, the encryption technique is used with is done using RSA algorithm.
After the whole process completed which is explained above, if client wants to upload the file, MD5 is generated and diagnosed. The file which is to be uploaded is divided into chunks and then ECC algorithm is applied for decrypting the file. The decrypted file will generate and will compare to the MD5 generated and diagnosed above. If there is no modification then the generated file is correct.

6. EXPERIMENTAL ANALYSIS

The proposed result shows the time variations between encryption and decryption. Below graph shows the comparison of time taken for encryption on authentication server using RSA algorithm and time taken for decryption on resource server using RSA algorithm.

Below is the graph showing the result of comparison between the token generation time on authentication server using RSA algorithm and token verification time on resource server using RSA algorithm.

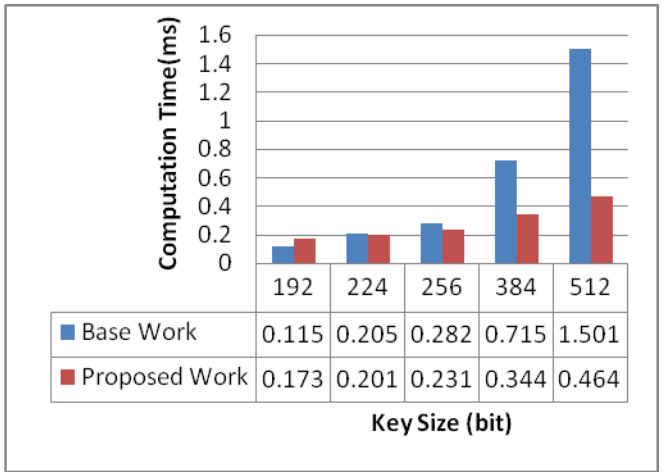

Figure 6: Authentication time comparison graph

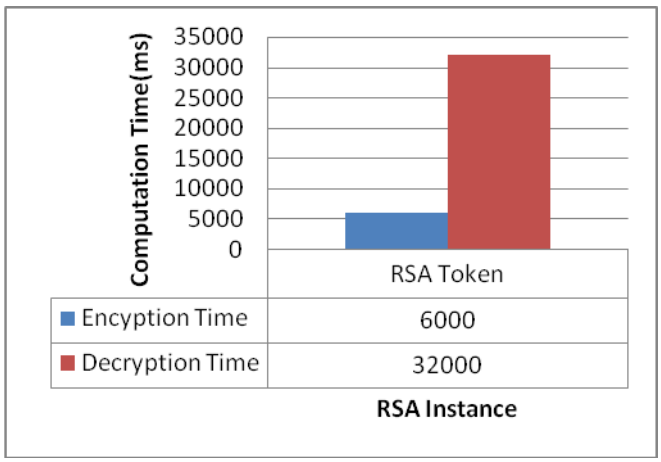

Figure 6: Comparison of Computation Time

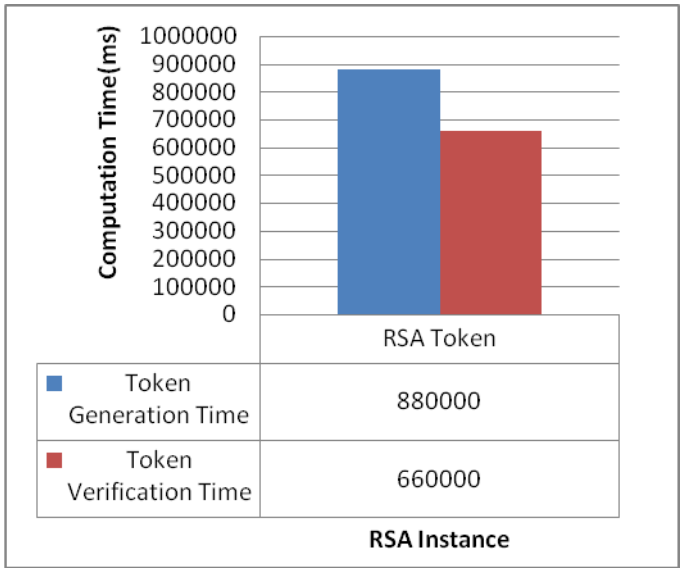

Figure 7: Comparison of Token Time

7. CONCLUSION

The complete observation concludes that the environment is created for storing, in secure manner. In the complete work we have discussed about security which can be implemented using Kerberos protocol along with RSA and ECC algorithm.

Many researches and study is done which describes that data loss and dependency on cloud vendors creates the loss of control on data loss. This approach of security using Kerberos authentication protocol is the better way and with the Kerberos protocol, RSA and ECC is also used, which will make it more secure. RSA and ECC here used for encryption and decryption using public key and private key. The complete work observes that the algorithm used are beneficial and through it, it can be concluded that on the basis of need of cloud, better security is implemented.

6. REFERENCE

1. Prof. Vishwanath S. Mahalle. “Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing”, International journal of pure & applied research in engineering and technology, 2013, volume (8):220-227, ISSN-2319-507X IJPRET.

2. Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) – 28-30 Oct, 2010 IEEE.

3. Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch:Rewining the World, from Edison to Google, , CITIC Publishing House, October 2008.

4. Ya-Qin Zhang, the future of computing in the "cloud-Client", The Economic Observer reported, http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri.

5. S. M. Chow, C. Chu, and X Huang,”Dynamic secure cloud storage with provenance.” Cryptography and Security: from Theory to Applications, LNCS, Springer, pp. 442-464, 2011.

6. F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. Kohpayeh Araghi, N. Morad Alibeigi, and S. Dabbaghi Varnosfaderani, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments,” in IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 2014, pp. 508–513.

7. S. Zarandioon, D.D. Yao, and V. Ganapathy, "K2C: Cryptographic cloud storage with lazy revocation and anonymous access", Security and Privacy in Communication Networks, Springer Berlin Heidelberg, pp. 59-76, 2012.

8. A. Abuhussein, H. Bedi and S. Shiva, “ Evaluating security and privacy in cloud computing services: a stakeholders perspective.”, Proceeding of: In Internet Technology And Secured Transactions, 2012, International Conference For, pp. 388-395. IEEE, 2012., At London, UK.

9. J. Varia, S. Mathew, (2013). “White paper: Overview of Amazon web services,” U.S: Amazon web services, inc., 2013.

10. G. Haff, “White paper: Why the future of the cloud is open,” Raleigh, NC: Red Hat, inc., 2012.