Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

Kerberos System to Cloud for Virtual Resource Authentication

N. Sundareswaran[1] A. D. C. Navin Dhinnesh[2] S. S. Akilan[3]
[#1,2,3] Department of Computer Applications
Mepco Schlenk Engineering College
Sivakasi

***Abstract* - The security of the virtual network will not benefit from using authentication method with the most promise for security unless both the way it is coded and the way it is implemented is equally as secure. It is essential to choose strong authentication algorithms which enforce good protection. The importance of the resource authentication process is the ability of the client to access and use the resource. A pseudo code was developed for the data center which is used to authenticate the client to use the resource. Our cloud infrastructure suggests using certificate based authentication for this sensitive access of the cloud. We can use encryption to protect stored passwords in the data center. We are using symmetric key algorithm, Advanced Encryption Standard with stretching the block size for this purpose. The data center does not keep all documents at one place. It keeps transposition the order of the documents in different virtual servers. There is no known attack for the Kerberos system till now which motivates us to involve this system to the cloud for resource authentication.**

Keywords:* *Virtual Network, Resource Authentication, Transposition, AES, Kerberos

I. INTRODUCTION

The layered security approach can be applied to the virtual server where security controls are placed to increase the amount of work required for an attacker to break down the defenses and reduce the risk of unintended failure of any single technology for example, We provide a layered segmentation approach in cloud security provides a useful conceptual model for administration in the data center . For example, the data layer and application layer communication to provide authorized systems. It has highest level of trust because the data layer house sensitive and confidential information which never be directly communicate to the internet only through application which is local to the data center. A trust model can be established in the data center to allow a broad view of networks, systems and VM communications and it distinguish boundaries between networks and VM systems [1]. Most of the cloud security software only authenticate at the start of a connection, so once the connection is established which allows unrestricted access directly from the internet. It is a type of internal threat of the data center. A general cloud security model is shown in figure 1.

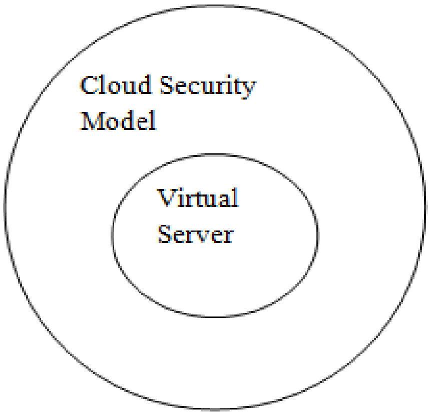

Fig1. Security Model

Risk analysis is an important part of any successful security effort and it should analyze and categorize the things to be protected and avoided. It should also provide a means to measure the effectiveness of the overall security architecture.

II. AUTHENTICATION

Data center cloud security needs stronger controls than the simple password. The security of the virtual network will not benefit from using authentication method with the most promise for security unless both the way it is coded and the way it is implemented is equally as secure [2]. An authentication typically suffers against three attacks such that dictionary attack – Attack uses same algorithm to hash words in a dictionary, heuristic attack – attack uses the things commonly do which predicts the password, brute force – attack checks every possible combination.

A. Strong Authentication

It is essential to choose strong authentication algorithms which enforce good protection. We can use encryption to protect stored passwords in the data center. We are using symmetric key algorithm (Advanced Encryption Standard) with stretching the block size for this purpose [3]. It works as the following procedure**.** It set the number of rounds as r such that each of the (b+y) bits as input where b is confined to block size and y is additional bits to speed up the process. XOR all (b+y) bits with key as the first step and multiple rounds of repeated operations such as bit shuffling, substitution boxes (s-box) and linear mixing using modular algebra. The following equation 1 is the AES general encryption method.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

$$E^{-1}_k\,(E_k(M)) = M \qquad (1)$$

where

M – Message Block
$E_k(M)$ – Encryption with key
E^{-1}_k – Inverse of the Encryption with key.

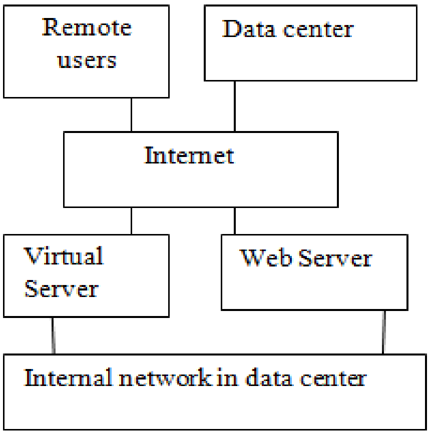

Fig 2. Trust Model

B. Remote user – Password Authentication:

Figure 2 shows the interconnection between the data center with user. The public key cryptography (RSA algorithm) is used to encrypt/decrypt the password. However it is subject to replay attacks. If the response can be captured, it might be used by an attacker to authenticate to the data center. So the encryption can be further strengthened by MD4 message digest. It is the result of cryptographic hash to the data (password) and we apply the encryption algorithm.

C. Data center resource Authentication:

The importance of the resource authentication process is the ability of the client to access and use the resource; which depends on the following two things.

1. Whether client can successfully authenticate to the data center, it was checked in network authentication system and obtain a service ticket?
2. Whether client is authorized to access the resource?

The client sends a request for the use of a specific resource; [3] the data center validates the request and examines the resource availability. If the resource is available, virtual server issues a service ticket for the requested resource. Part of the ticket is encrypted using the credentials of the service (the password for the computer system on which the service lies) and part of the ticket is encrypted with the credentials of the client.

D. Non repudiation

It is the guarantee that something came from the source it claims. It means that the data center is responsible for data integrity. Digital signature can be produced using public key cryptography. It works as follows, the password is hashed to produce digest. This digest is encrypted using private key of the client then data center would receive this encrypted digest and virtual server would decrypt the digest using client's public key. If this public key can decrypt the digest then it is certain that integrity has been proved.

E. Authentication for an organization

An organization can claim to manage all of their user accounts which include change settings, monitoring, and resource usage. The client can decrypt its part of the ticket and thus knows what resource it may use. The client sends the ticket to the resource computer along with a fresh timestamp. The resource computer validates the timestamp by checking whether the time is within the valid period and then decrypts its portion of the ticket [4]. This tells the computer which resource is requested and provides proof that the client has been authenticated.

F. Certificate based authentication

Our cloud infrastructure suggests using certificate based authentication for this sensitive access of the cloud. A certificate is a collection of information that binds an identity (user, computer, service) to the public key [4]. Each certificate's public key has its associated private key which is kept secret. Authentication works as follows, the client issues request as super user (organization) then data center issues a challenge (random number) and client application uses its private key to encrypt the challenge and then the response of this process is returned to the data center. Since the data center has a copy of the certificate, it can use the public key of the client to decrypt the response. The result is compared to the challenge, if there is a match, the client is authenticated.

G. Secure Communication with data center

It is essential to provide authentication of secure web servers and clients to share things. [2] The advantage is that the identity of the virtual server in the data center can be proven by the client. Client and virtual server share an encryption key that can be used to secure communication between two of them.

The client request for the web page which is present in the data center and server sends its certificate to the client then client checks its certificate issued by public certificate authority. The client validates the certificate by checking the signature using public key. If the test is successful, the client accepts the virtual server certificate as valid.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

PSEUDO CODE

```
Input: Certificate, Cipher text (digitally signed)

If check (cert, client lists) matches then
    Source is authenticated
    Call Decrypt( cipher, pub_key_client)
    If decrypted password matches the client then
        Client is authenticated.
    End if
Input: Client Request for Resource
Data center issues service ticket (st).
Compute P= s/2 where p1=s/2, p2=s/2
(divides the service ticket by two parts)
Function call Encrypt ( p1, p2)    // where p1 is
encrypted by server's key and P2 is encrypted by
client's key.
Call send ( c, st)      // service ticket is sent to
//   client.
Call decrypt ( st,pr_key_c)    // p1 is decrypted
//and will be sent to ds.
call decrypt (st,pr_key_ds)   //p2 is decrypted
//using private key of ds.
if (check ( request, access_control))  then
    request is authorized.
else
    request is not authorized.
END
```

The Pseudo code for cloud authentication, authorization was discussed above.

III. CLOUD AUTHORIZATION

There are varieties of types of authorization including client rights, role based authorization, access control lists and rule based authorization. Virtual servers are divided into client space, kernel space and ability to use in one space or the other is strictly controlled. Generally in data center, the ability to create groups, assign users to groups, log on to a system and many more rights can be assigned.

A. Role based authorization

A client (or) organization can assign individual virtual machines to their members (or) users. A particular user (or) virtual machine can include the role of auditor who can read activities of the other virtual machines (or) members but not modify or perform other role in their machines and members are allowed to perform only specific applications [5]. We can apply a security model to the cloud. In this model virtual machines are divided into zones. Data may not be moved from zone to zone without special authorization. Access control lists provide the list of authorized virtual machines which are authorized for different communications like resource request, file request and network device request.

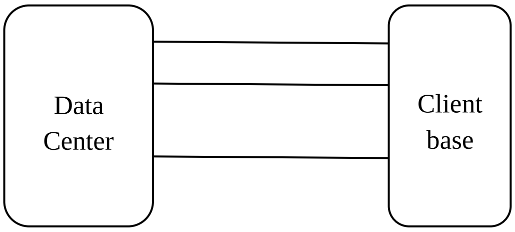

Fig 3. Cloud Security base

IV. DATA SECURITY ON CLOUD

Each bit of data can be accurate and ready when needed. As shown in Fig 3, client and data center is strictly connected by more than one virtual layer. In cloud keeping data secrets by disguising them, hiding them or making them indecipherable to others is good practice. The data is obscured using algorithms and secret keys. Generally it is difficult to decipher the meaning of a document if it is written in a language we do not know. The data center does not keep all documents at one place. It keeps transposition (rearrange) the order of the documents in different virtual servers [6]. The name of the document itself gets changed using substitution method. This substitution algorithm replaces each character in a document with another.

A. RSA Algorithm

We have used RSA algorithm for data authentication because brute force key search is not possible for given input size n (length of password), mathematical attacks also suffer to factor modulo N. Timing attacks also impossible due to our Kerberos system [7]. The overview of procedure as follows.

We need to select primes p, q then compute n= (p-1) (q-1) hence determine de=1 mod n, d<n and choose to publish public key as KU= (e, pq) where e is a random prime number and secret private key KR= (d, p, q) where d is secret number.

RSA takes O ($e^{lognloglogn}$) operations due to factorization; it is very hard to break.

V. ADMINISTRATIVE SECURITY

Cloud administrator is the one who perform back up, database administration, maintenance and even help desk support on remote all have elevated privileges within the data center as shown in fig 4. To ensure the security, we must consider the controls that can prevent administrative abuse on privilege.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

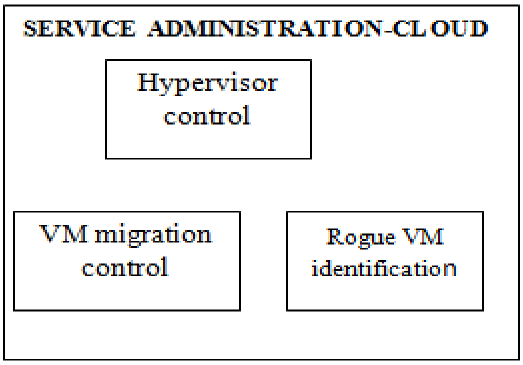

Fig 4. Cloud Service Administration

VI. RESULT ANALYSIS

Most of the cloud security software only authenticate at the start of a connection, so once the connection is established which allows unrestricted access directly from the internet. Then the resource authentication process starts, it is the ability of the client to access and use the resource. When client can successfully authenticate to the data center, it was checked in network authentication system and obtain a service ticket. Now the client is authorized to access the resource. The pseudo code explains the actual process. Our cloud infrastructure suggests using certificate based authentication for this sensitive access of the cloud. A certificate is a collection of information that binds an identity (user, computer, service) to the public key. Each certificate's public key has its associated private key which is kept secret. the data center is responsible for data integrity. Digital signature can be produced using public key cryptography. We can apply a security model to the cloud. In this model virtual machines are divided into zones. Data may not be moved from zone to zone without special authorization. Access control lists provide the list of authorized virtual machines which are authorized for different communications like resource request, file request and network device request. The data center does not keep all documents at one place. It keeps transposition (rearrange) the order of the documents in different virtual servers. The name of the document itself gets changed using substitution method. This substitution algorithm replaces each character in a document with another. We use AES symmetric key algorithm for encryption of file.

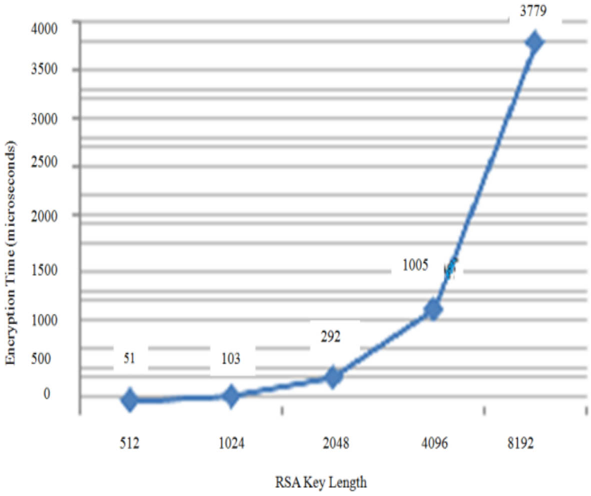

Fig. 5 Relative time with respect to key length

VII. CONCLUSION

It is important to choose strong authentication algorithms and authorization method which enforce good protection. We have used AES encryption with stretching the block size to protect stored passwords in the data center. Network authentication system is used to authenticate the client which had no known attacks till date. The pseudo code is implemented for resource authentication. Client is forced to send its certificate for further identification. Digital signature is used to ensure the integrity of the client. Access control lists are strictly followed for the clarity of the authorization. We have used RSA algorithm for encryption/decryption to apply strong authentication from both side. Figure 5 shows the relative time with respect to key length of the data size [8].

REFERENCES

[1] Virtualization Security and Best Practice, Rob Randel CISSP, Reference Book copy.
[2] Network Security by Roberta Bragg, Mark Rhodes-Ousley, Keith Strassberg, Tata Mcgraw-Hill
[3] Flexible block cipher design to stretch the block size of the block ciphers, Sundareswaran N, ASNET National Conference, PSNA College of engg, Dindigul
[4] Network Security, The Complete Reference, Robertta Bragg, Book guide.
[5] User Privacy and Security in cloud computing, Al Museelem Waled, Reference Book material.
[6] Cloud Security, a comprehensive guide to secure cloud computing by Ronald L.Krutz and Russell Dean Vines, Wiley Publication
[7] The RSA algorithm based on the idea factorization of integers, www.cse.nthu.edu
[8] Performance analysis of cryptography methods for securing message exchanging in VANET, Ali Mohamamadi, A.A. Pouyan, International Journal of Scientific and Engineering Research, Volume 5, issue 2, Feb 2014

(This work is licensed under a Creative Commons Attribution 4.0 International License.)