IJRSET Volume 2, Issue 3 Pages: 8-11

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

SECURITY of CLOUD STORAGE: NAC, TLE and VPD APPROACHES

[1] Khan Ibna Nayas, [2] Badhan Saha Setu

[1] Department of Computer Science and Engineering, Daffodil International University
[1] House no-29, Flat no-25, paikpara govt staff quarter, mirpur-1, dhaka-1216, Bangladesh
[2] Department of Computer Science and Engineering, Daffodil International University
[2] House no-43, 6th floor, F-3 Sukrabad, dhaka-1207, Bangladesh

Abstract:-

This is the age of Information Technology (IT). The cloud computing are the biggest concept in this era and another core concept than cloud computing is that security of cloud storage. Without security of a system is like as a boat without rudder. In this time there are lot of system and method which make our life easy but security of that system is the major question. In this time the lack of security is vast problem in our life. Many resources and data are hacked day by day. So, security is the most important matter in our technology. The Network admission control (NAC) protocol is an end point device technology and solution which is provided by Cisco. It is also called Cisco NAC. NAC identifies all build up a strong security self-depending network and gives an extra performance. This paper describes how to NAC allows trusted endpoint devices and deny the access of unauthorized devices in a network or network zone. The Two Layer Encryption (TLE) techniques are that provides the extended secure communication. And the virtual Private Database (VPD) is a concept of oracle that allows the DBA (Database Administrator) to control access to data in the database. It is secured all user information row and column level so that nobody cannot see the user's data Except DBA (Database Administrator) in this system.

Keywords: - NAC, TLE, VPD, RADIUS server, Access-FGA.

1. INTRODUCTION

The Network Admission Control (NAC) is a part of the Cisco self-depending network initiative, which helps identify, prevent, and build up an extra-large security for all kind of network.

The NAC works likes as antivirus and desktop management.

For using NAC, the endpoint device has some software that manages willingness.

The unauthorized person hack the information in many portion of a network and server. They choose the network device (such as router, switch, access point etc), transmission medium, gateway of a network, and server etc.

The NAC ensure security of that case except the data transmission case. In this case we use the two layers Encryption technique (TLE) for protect the user data as in ([10], [11]).

In two layer encryption technique we use two valuable methods they are ACL and Caesar cipher encryption technique. The ACL protect the network layer and Caesar cipher protects the data in presentation layer as in [8].

In cloud security we use Virtual Private Database (VPD) which secures all users' data in row and column level in cloud server.

2. BACKGROUND

NAC is build up by Cisco day by day with many steps. Some of those major steps describe below.

A. First step

NAC framework release 1.0 (formerly referred to as first phase) become available from Cisco Systems in June 2004 with many layer 3 Cisco network access devices as in [12].

B. Second step

In October 2004, Cisco acquired prefigures clean machines and added it to the NAC technologies options. This technology was renamed Cisco clean access and then NAC Appliance in2005 as in [13].

C. Third step

In November 2005, NAC frameworks release 2.0 became available and added even more features, including more NADS that work at layer 2 and more protocols as in ([14], [15]).

D. Fourth step

The background of TLE is single layer encryption (SLE). It is using before two layer encryption. In SLE, the data owner to enforce all the ACPs by fine-grained encryption technique as in ([1], [2]).

E. Fifth step

The Virtual Private Database (VPD) is a new concept for cloud computing and cloud security but before it is use in oracle as in [9].

1. CASE STUDY

For building security on campus network and cloud storage, we implemented NAC as end point device security, TLE for ensure secure communication and VPD in cloud storage data security. Those protocols are more important for cloud and end point device and data security.

A. Case one

NAC works as authentication protocol. We use three powerful server which named AAA server, RADIUS server, and TACACS server for authentication and authorization. When a user or person enter the network or send an EAP message to AAA server then the server send it to RADIUS server. RADIUS server check the user is authorized or not then the RADIUS server sends it to TACACS server for again checking authorization. If the user is authorized then the DHCP server through an IP for communication with all host in the network.

B. Case two

TLE (two layer encryption) technique is secure two layer of OSI reference model. We use Caesar cipher algorithm for secure presentation layer and ACL (access control list) for secure Network layer ([1], [2], [7]).

C. Case three

VPD is a concept of ORACLE which we implement in cloud server. This protocol secure data row and column level. When a user shows his own data then he has to login the correct username and password. So every user's data is protected.

3. PROPOSE SYSTEM

Based on our thesis, we propose a system for NAC is the end user or a whole corporate network security, TLE is the data security when it is transmit sender to receiver, and VPD is a kind of server security for cloud. The whole system describe a user when request the server to enter that network, the NAC server check the user is authorized or not. If it is authorized then it is enter that network and when send the user when store data in system server then the VPD secure data from any other user or unauthorized person. In

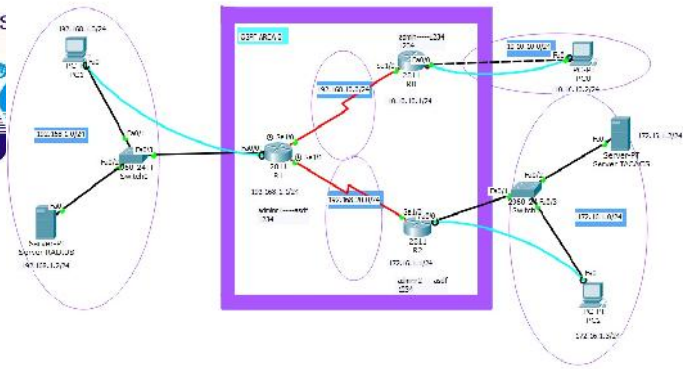

Figure 1: Configuring NAC with RADIUS and TACACS server

NAC, we use three servers for authentication and authorization. They are AAA server, RADIUS server, and TACACS server. When a request is found then the router send it the AAA server verify the authentication and authorization, when AAA server found it is authorized then AAA server send it RADIUS and TACACS server to again check this authorized host ([3], [4], [14]). When all checking is finished then AAA server request the DHCP server to give the ip for the requesting host then the DHC server send an ip address [5]. And TLE, we use Caesar cipher data encryption technique from symmetric cipher model [6]. In VPD, we use oracle virtual private

database which secure user data in row and column level [9]. So, whole system is secure user end point to server level in all kind of big, small, or any corporate networks.

CONCLUSIONS

Now a day's security is the major factor for all institution and every person. In network and data security the Network Admission Control (NAC) protocol is a large security protocol for end user, small or big network, campus network and organizational network. It is ensure security using configure many kind of valuable server as like as Basic AAA server, RADIUS server, TACACS server etc. The main application feature of NAC to ensure security is User Identification, Compliance and Enforcement. The another security protocol for presentation layer and network layer is Caesar cipher encryption technique and access control list(ACL) respectively, which ensure data and network security when data is passing. The virtual Private Database (VPD) is a great concept of oracle which is ensures the server and database security. It is secure user data in row and column level so that nobody cannot see other's user data. It means the every user see his/her own data but not seen another user data. So, whole system is secure when using those three concepts in a network and storage. Now we propose this system that we secure data from hacker and third party but we store our data in cloud service provider as like Google, Amazon and another company. The admin of cloud server can read or write the data because of Caesar cipher isn't a strong encryption technique. In future, we will works about AES & RSA replacement of Caesar cipher and invented a system that, the admin of cloud service provider and hacker all people cannot see and read the data and provide another extended security system. Because Advanced Encryption Standard (AES) and Rivest, Shamir and Adleman (RSA) is one of the most frequently used and most secure encryption algorithms available today.

4. ACKNOWLEDGMENT

This research paper is made from the help and support from everyone, along with: Parents, educator, family, friends, and in substance all perceptive beings. Especially, allow and support me to dedicate my acknowledgement of gratitude toward following effective advisor and inspiration person:

First, I would like to thank Dr Syed Akhter Hossain for his most amazing support and inspiration. Second, I would like to thank Narayan Ranjan Chakraborty to read my thesis paper and to provide valuable advices for the paper. Finally, I sincerely thank to my parents, family, and friends, who provide advice and financial support. The product of this research paper would not be possible without all of them.

REFERENCES

[1] William Stallings, Cryptography and Network Security, 4th ed., Pearson Education Inc. and Dorling Kindersley Publishing Inc., 2006.
[2] William Stallings, Cryptography and Network Security, 4th ed., Pearson Education Inc. and Dorling Kindersley Publishing Inc., 2006.
[3] (2013) The Cisco website. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/securityvpn/remote-authentication-dial-user-service-radius/13838-10.html
[4] (2014) The Cisco website. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/securityvpn/remote-authentication-dial-user-service-radius/13838-10.html
[5] (2014) The Cisco press website. [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=170744&seqNum=4
[6] (2015) The Wikipedia website. [Online]. Available: http://en.wikipedia.org/wiki/Encryption
[7] (2014) The Microsoft website. [Online]. Available: http://technet.microsoft.com/enus/library/cc962027.aspx
[8] (2014) The Tec target website. [Online]. Available: http://searchsoftwarequality.techtarget.com/definition/access-control-list
[9] (2014) The Tec target website. [Online]. Available: http://searchoracle.techtarget.com/definition/virtual-private database-VPD
[10] (2014) The Wikipedia website. [Online]. Available:

http://en.wikipedia.org/wiki/Network_Admission_Control
[11] (2015) The Network world website. [Online]. Available: http://www.networkworld.com/article/2209370/security/nacstandards-wars-end-in-truce.html
[12] (2014) The IETF website. [Online]. Available: https://www.ietf.org/rfc/rfc5792.txt
[13] (2014) The IETF website. [Online]. Available: https://www.ietf.org/rfc/rfc5793.txt
[14] (2013) The Microsoft website. [Online]. Available: http://technet.microsoft.com/enus/library/bb457015.aspx
[15] (2014) The Wikipedia website. [Online]. Available: http://en.wikipedia.org/wiki/AAA_protocol