Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Security of Private Cloud with Log Analysis and Encryped Channel

Kuntal Shah
M.Tech Cyber Security
Raksha Shakti University
Ahmedabad, India

Prof. Chandresh Parekh
Department of Telecommunication
Raksha Shakti University
Ahmedabad, India

Asst.Prof. Bhadresh Gohil
GTU P.G.School
Gandhinagar, India

Abstract: With the help of private cloud it is easy to share the files, folders and mails in private network. Current security techniques just encrypt the file with password and share the password with another channel, but guessing of password is the main attack in this type of system. Sometimes due to the unencrypted channel man-in-the-middle attack is also possible. Another main problem is automated scanners which are used to find the vulnerability in the system and exploitation. So there is a need of system which can resist to the attacks like man-in-the-middle, denial of service and password guessing. We have suggested log based analysis method which will protect the system from the attacks like denial of service and password guessing and automated scanners. We are also using encrypted channel so that attacks like man-in-the-middle cannot be possible.

Keywords: Asymmetric cryptography; Cloud; open Source; Software based key generation;

I. INTRODUCTION

With the help of the private cloud it is easy to share the files but as every technology has its own pros and cons the private cloud with internet has also its vulnerability. For any security system the main need is Privacy, Authenticity, Integrity and Non-repudiation (P.A.I.N).[1]

Privacy relates that data or file being transferred cannot be accessed by the unauthorized parties. Authenticity relates that the authenticated person only should be able to access the data. Integrity relates to the data is not modified by the unauthorized parties when data is in transit. Non-repudiation means the sender should not able to deny that message is sent by them.[1][2]

Traditionally files were sent without encryption but due to security concern the encryption of file came in picture. To secure the private system there were many cryptographic algorithms had been developed.

There are mainly two types of cryptographic systems are used based on their key distribution system. The mainly used encryption system is **symmetric key** based encryption system where the sender and receiver are using the same key to encrypt and decrypt the file and communication. The main problem is that those who have the key can decrypt the message.[2] Main problem of this type of cryptographic algorithm is sharing of key. So for secure transmission of the key one extra communication channel is used to share the key. But the main problem is it is easy to crack this password with brute force attack and man in the middle attack. [3] The main advantage of the symmetric key cryptography is it gives better privacy but it is not capable to solve the issues like authenticity, integrity and non-repudiation. [4] So there is a need of new type of authentication system that can provide authentication that the client or user is authorized, integrity of file is maintained and the non-repudiation. The perfect solution for P.A.I.N is Asymmetric key based encryption system with digital certificate and digital signature. [5] The concept of the digital certificate is widely used by server to authenticate client. The mainly used this type of scheme is known as SSL or TLS services. The main problem in this type of system is the generation and the distribution of the key.[6] Many organizations have provided hardware based solution of it but it is not scalable. In this paper we have given the solution for the file transmitting service which is based on asymmetric key cryptography and is scalable for the large user and completely software based key generation. This system will transfer the file in encrypted form so that the intruder cannot be able access it.[7][8]

II. PRAPOSED ALGORITHM FOR AUTHENTICATION

To overcome the problem of the private cloud we have proposed a more secured cloud based file sharing system framework that is more resistant to different attacks. Figure1 shows the flow of the security system. The basic work flow is as given below:

- Browser based File sharing System or cloud
- To create a secured transmission channel
- Minimize the attack possibilities by differentiating between legitimate traffic and automated traffic.
- To create a secured authentication system
- Server side encryption

As shown in the Flow chart when the user want to access or share the file he/she will send the request through the browser.

System will check whether the traffic is HTTPS or not, if the traffic is not https than it will provide SSL certificate and converts to the https. Due to this the client will receive a SSL certificate which will provides the authenticity of the server to the client and channel will be encrypted so that the data is safe in transmission. [9]

Next step is to find whether the traffic is legitimate or not. For this we have suggest a log based method. If the scanners like NMAP is trying to scan the Cloud server than the logs like given in figure2 is generated. So if we make any script that can automatically detect this type of attack than this host can be banned. We are using same methods to protect the

system from the denial of service attack. We can limit the attacker that if its requesting more than predefined attempts than it will be blocked.[10]

We can define Denial of Service attack by searching the text

” %(__prefix_line)sDid not receive identification string from <HOST>\s*$”

And by modifying firewall rules we can ban that IP address.

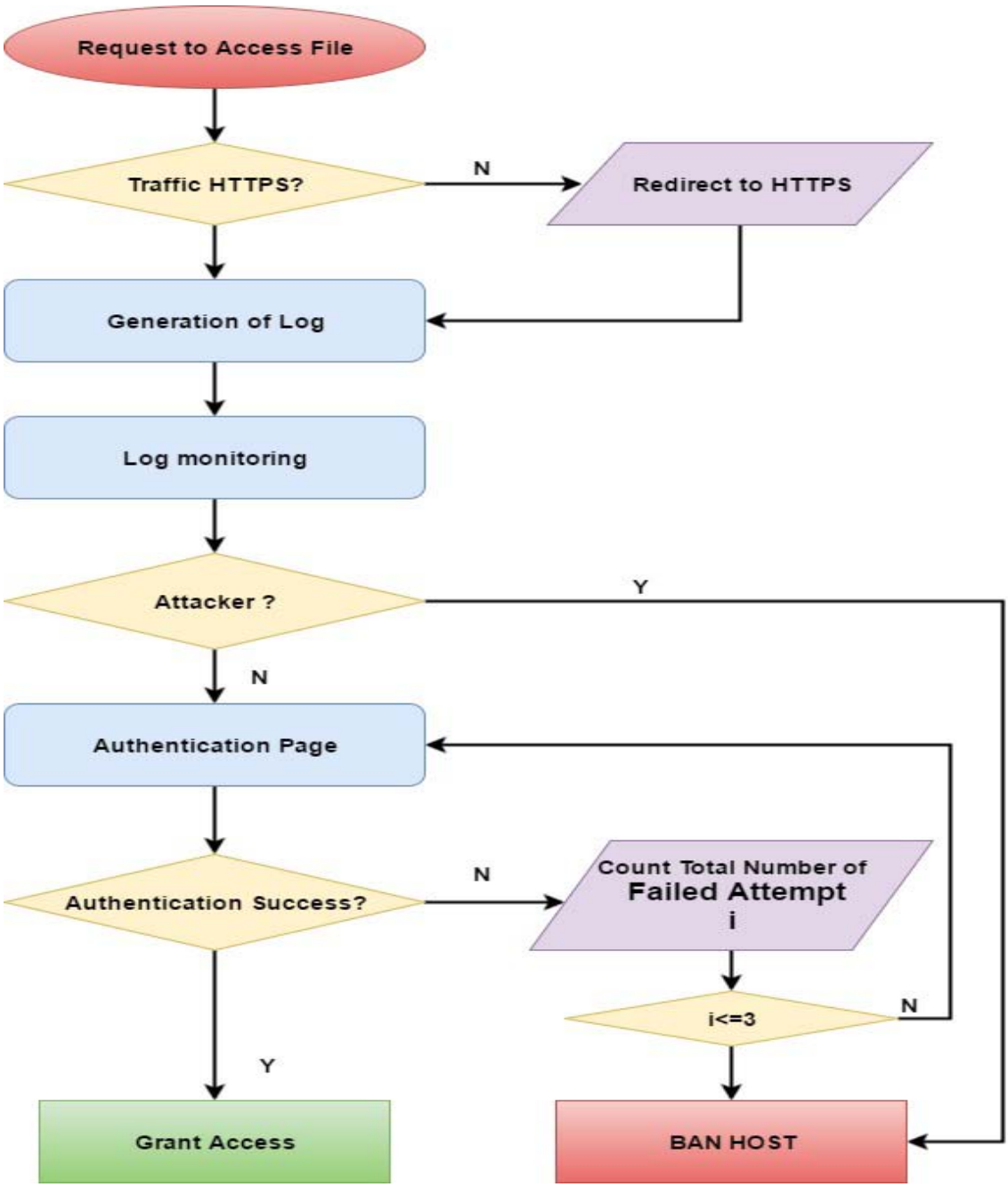

Figure 1: Flow Chart

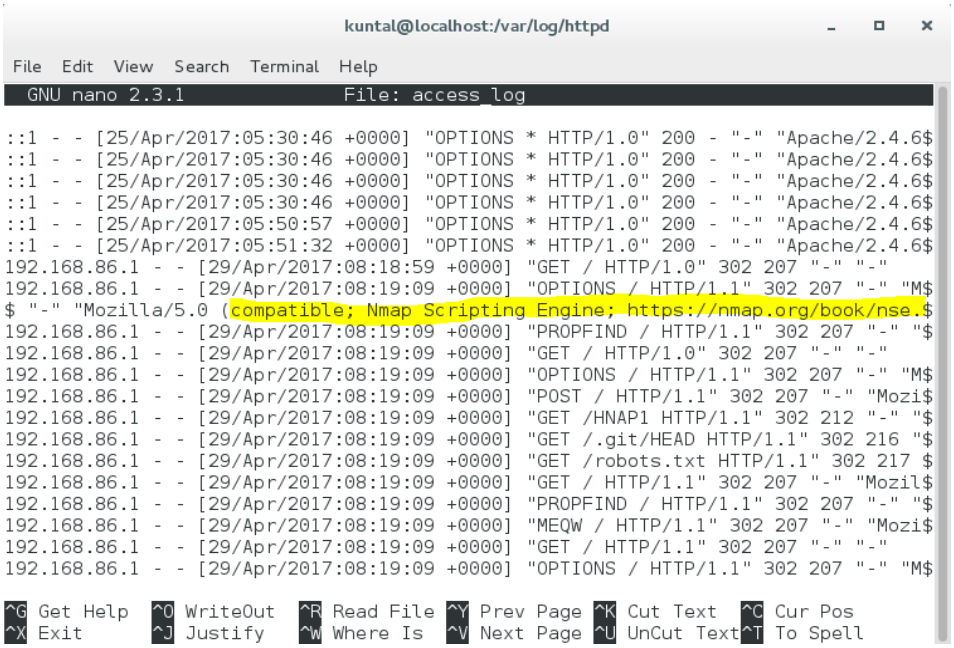

Figure 2 : Apapche Access Log

To find the authenticity of the user we have made a data base in which the user name and hashes of passwords were saved. Password is generated through the asymmetric key based password generation and authentication technique which cannot be breakable. To protect the system from the password guessing attack we can monitor the logs of failed attempts and if the failed attempts are above the predefined limit than ban the host.

There should be a system by which automatic log monitoring is possible, so that if there is any intrusion is detected than it can be banned. Like if any attacker tries to send many request at a time, tries to scan the website than it should be banned.

Our next step is to validate the user so that there is a data base created in server which stores the users and their passwords hashes. When client want to access their account they have to enter the correct user name and password. As shown in the flowchart total no of failed login attempts are counted, so that if the number of failed attacks are increases than predefined limit than that user should be banned and only authorized user can able to take access.

To protect the file in way that administrator can also not view the data we can use the same asymmetric key based encryption method by using user's password as a key and encrypting files in server. So user having correct key can only view the sensitive data.

V. RESULT AND ANALYSIS

Attack 1: Password guessing:

For the implementation purpose we are using ownCloud [11] as public cloud system and the Fail2Ban for automatic log analysis.[12] Ip of ownCloud is 192.16.224.130.

172.16.224.1 is an attacker's IP address which tries to enter different password and username to get the correct Username and password. Figure 3 shows the attacker's machine trying to add different passwords.

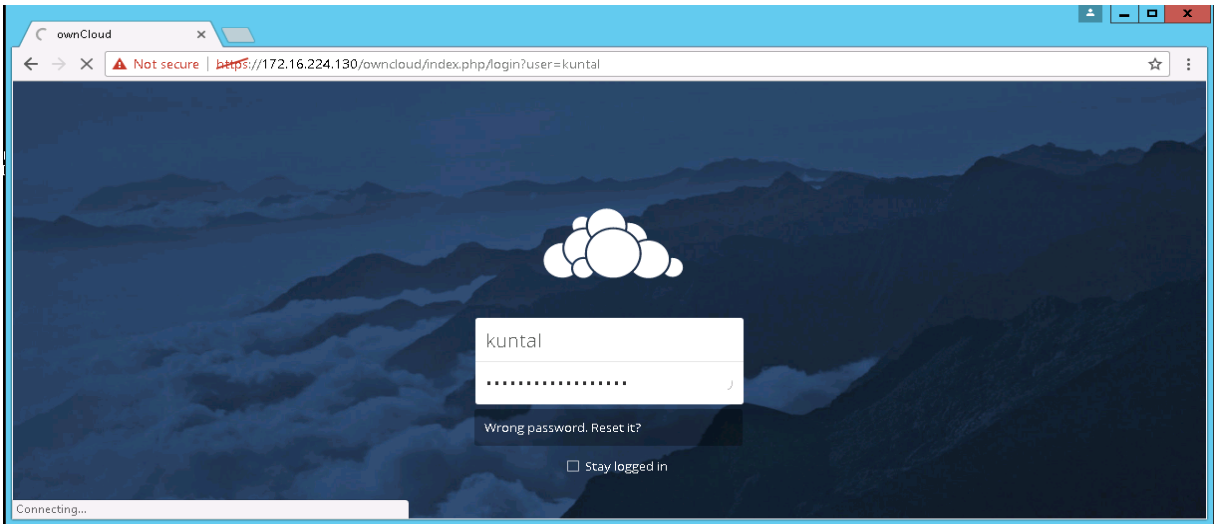

Figure 3 : Attacker trying passwod guessing attck

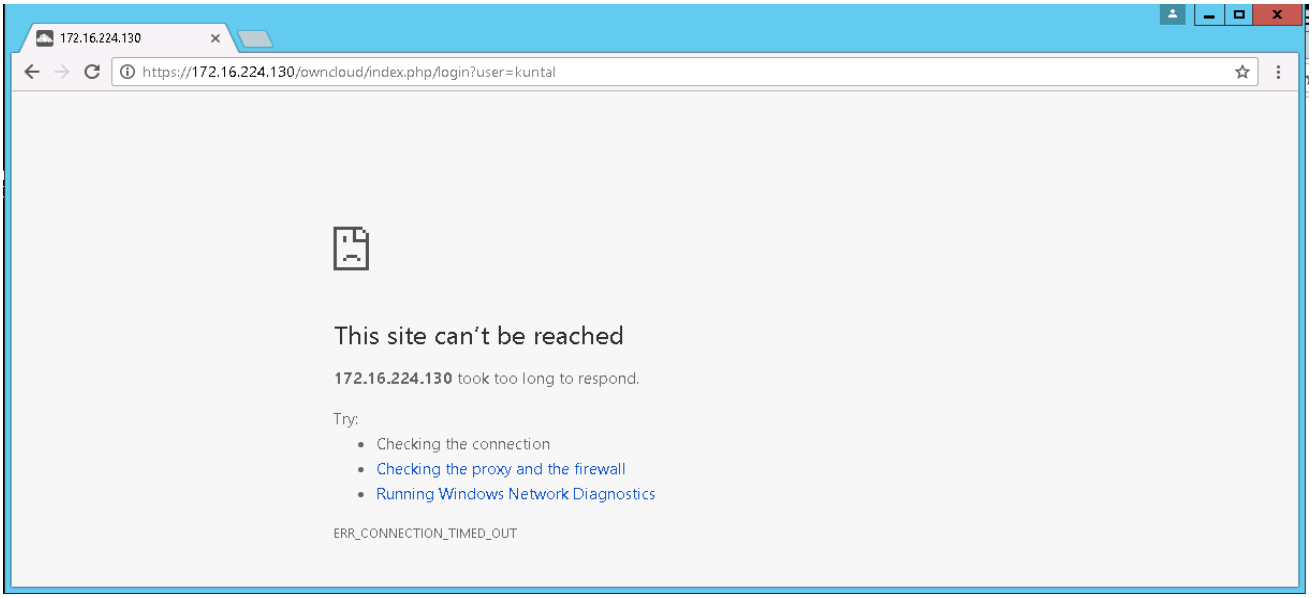

Figure 4 : BannedAttackers IP

Figure 4 shows the service of the attacker machine is banned.

Attack 2: Scanning of server's IP:

Figure 5 shows that the automated scanners will give the information about ownCloud server hosed on IP 192.168.86.139.

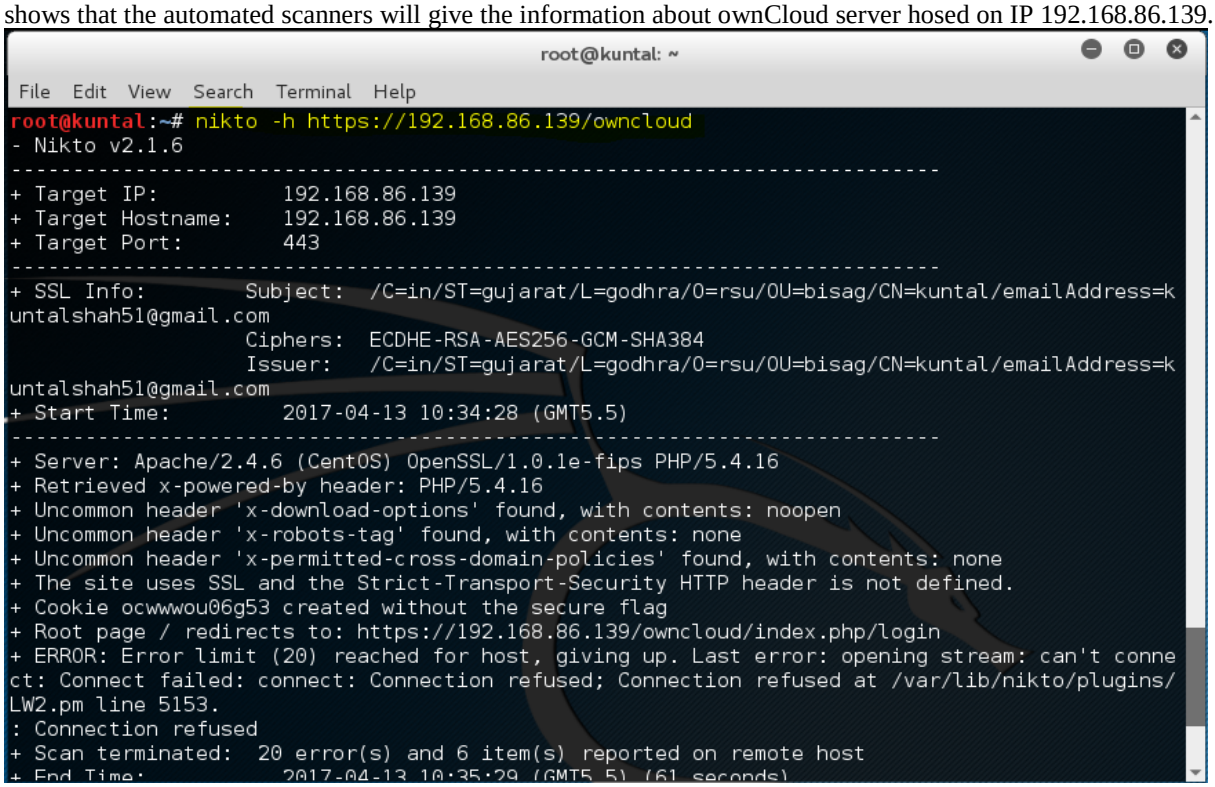

Figure 5: Scanning Result

Figure 6 shows that after automatic log analysis and firewall rule setting the IP of attacker will be banned and will not get any result shown in figure 6.

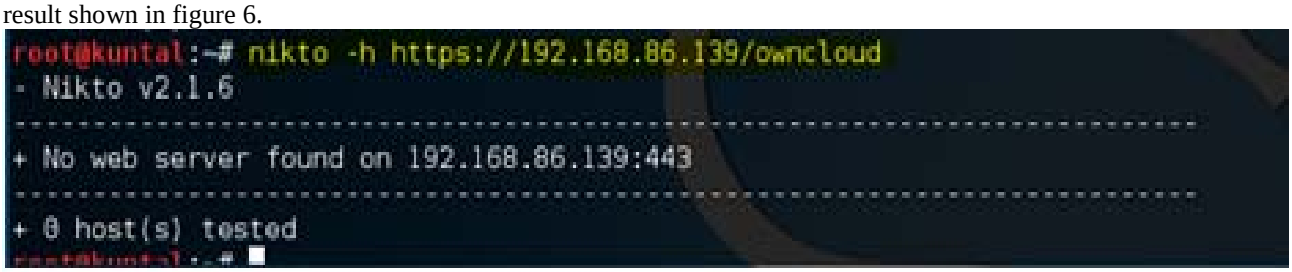

Figure 6: No scanning is possible

Attack3: Man-in-the-middle:

The data travelling between the machines is encrypted so that cannot be disclosed to the middle men or intruder. Figure 7 shows the encrypted traffic.

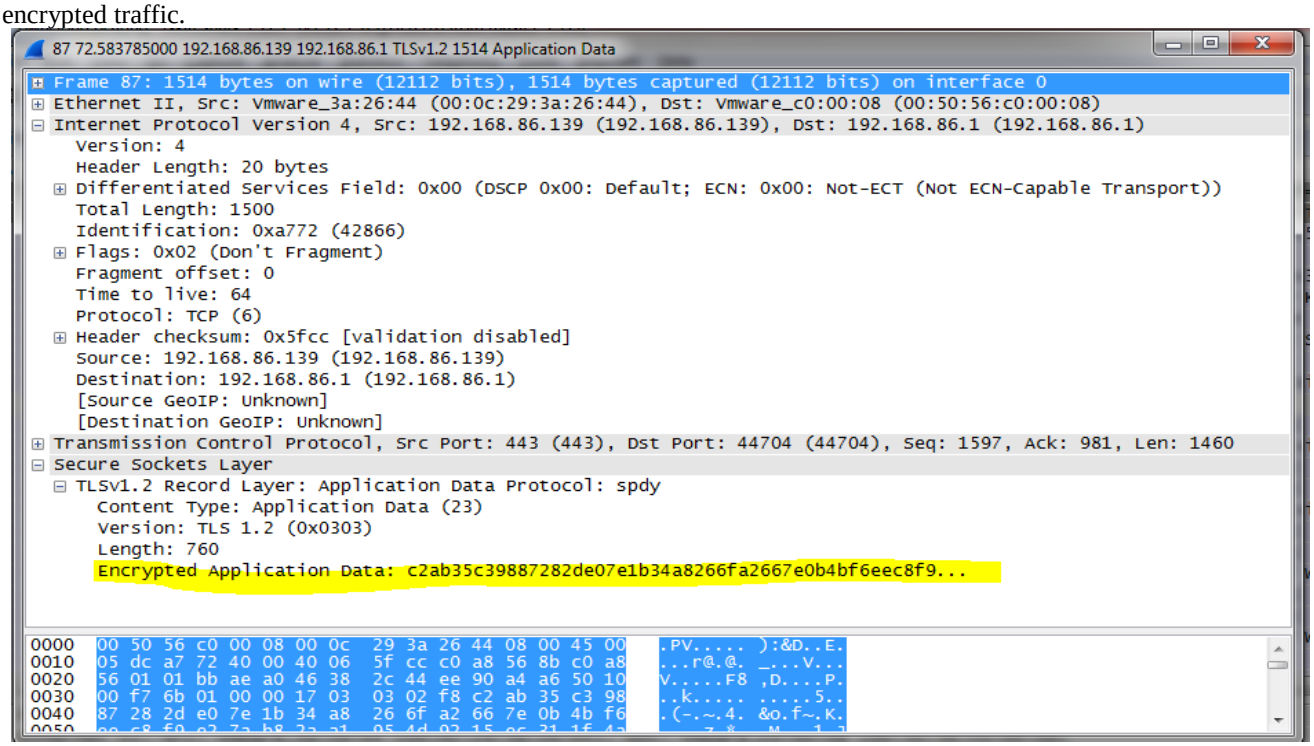

Figure 7: Encrypted Data in Transmission

Now if the user is legitimate he/she will allow using the service like shown in figure 8 which shows the admin panel.

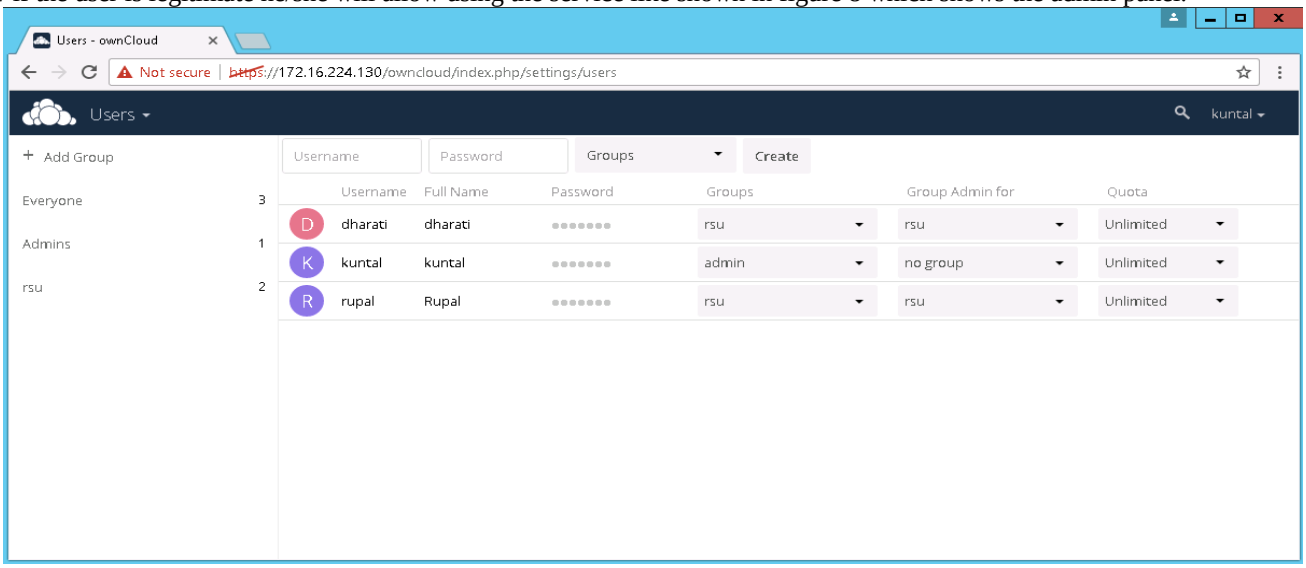

Figure 8: User Access

VI. CONCLUSION

Private Clouds are very useful in sharing the files and mails easily but it is not secure due to improper configuration and security loopholes. These vulnerabilities makes system unauthorized access of the file which can be very harmful for any organization. We have tried to give a log based solution to prevent the attacks like Password Guessing, Denial of Service attack and Scanning with automated tools. The secured channel will not allow passive attack like information gathering through channel.

REFERNCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", US Nat'l Inst. of Science and Technology, 2011

[2] Singh, S Preet and Maini, Raman. "Comparison of Data Encryption Algorithms", International Journal of Computer Science and Communication, vol. 2, No. 1, January-June 2011, pp. 125-127.

[3] Elminaam, D S Abd; Kader H M Abdual and Hadhoud, M Mohamed. "Evaluating the Performance of Sysmmetric Encryption Algorithms", International Journal of Network Security, Vol. 10, No. 3, pp. 216-222, May 2010.

[4] N. Gura, A. Patel, A. Wander, H. Eberle, S. Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", CHES, August 2004.

[5] A. Khalique, K. Singh, S. Sood, "A Password-Authenticated Key Agreement Scheme Based on ECC Using Smart Cards", International Journal of Computer Applications, vol. 2, no. 3, pp. 26-30, 2010.
[6] R. L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM Magazine, vol. 21, no. 2, pp. 120-126, 1978.
[7] W. Stallings, "Cryptograpy and Network Security Principle and Practice" in , Prentice Hall, 2011.
[8] M. Strebe, "Network Security Foundations" in SYBEX Inc., San Francisco, London:1151 Marina Village Parkway, Alameda, CA 94501, 2004
[9] Justin M. Beaver, Christopher T. Symons, Robert E. Gillen, "A Learning System for Discriminating Variants of Malicious Network Traffic", 8th Annual Cyber Security and Information Intelligence Research Workshop, October 30-November 2, 2012.
[10] J. Owens and J. Matthews, A Study of Passwords and Methods Used in Brute-Force SSH Attacks, USENIX Workshop on Large Scale Exploits and Emergent Threats (LEET), 2008.
[11] https://owncloud.org/
[12] Fail2ban, http://www.fail2ban.org