RESEARCHERID
THOMSON REUTERS

[Saxena, 6(8): August 2019]
DOI- 10.5281/zenodo.3367428

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

KERBEROS AUTHENTICATION MODEL FOR DATA SECURITY IN CLOUD COMPUTING USING HONEY-POT

Ms. Apurva Saxena*[1] & Dr.Anubha Dubey[2]

ABSTRACT

A honey pot is a technique of cloud computing that is proposed for capturing hackers or tracking unusual methods of attack. This technique will seize, recognize and duplicate the hacker behavior. It works in a Cloud environment where anything like technology, tool, and the result can be offered as a service. Purveyors offer and deliver such services to their customers via the network. This paper presents the concept of a high-interaction honeypot, Kerberos authentication system as a service in a cloud environment to implement the benefits of, such service to ably distinguish between hackers and users and to provide overall security to the data/network.

Keywords: *Honeypot, Kerberos, Cryptography, Cloud, Network.*

I. INTRODUCTION

Cloud computing is complete new technique put ahead from industry circle, it is the development of equivalent computing, distributed computing, and grid computing,[5] and is the amalgamation and development of virtualization, utility computing, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service(PaaS) and Software-as-a-Service (SaaS) [6]. Types of cloud services are IaaS (Infrastructure as a Service) in this client can get the infrastructure and virtual machine, networks on rental fee. PaaS (Platform as a Service) it is designed to build a platform for the user to expand a web or mobile apps without applying setup behind it [35]. SaaS (Software as a Service) it is designed to develop software for the user. IBM cloud works on all the services of the cloud. Cloud provider host and manages the application, underlying infrastructure and handle maintenance too.

Cloud computing is a model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing funds that can be quickly provisioned and released with negligible management effort or service provider interaction. To users, cloud computing is a Pay-per-Use-On-Demand mode that can opportunely access shared IT resources through the internet [14]. Where the IT resources include network, [5] server, storage, application, service and so on and they can be organized with much rapid and easy manner, and least management of and communications with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Virtualization is a solution point in the cloud system that provides multiple virtual illustrations of a physical resource and if a single instance of a resource is vulnerable then connected patrons get affected [7].

In cloud computing security is an important part. It is the combination of technologies and policies to protect the data, services, and infrastructure. This mixture is an objective of all possible attacks. Here we are using honeypot to trap the attacker securely so that repetition of attack can be avoided. A honeypot is designed for trapping hackers or tracking unconventional or new methods of hacking. Honeypots are used to identify vicious behavior performed over the Internet. If an attacker tries to invade or penetrate in the network by connecting this technique honeypot will ambush, detect and draw its activities. It is designed in such a way that if anything thrown at them will confine whether it may be a tool or strategy. Honeypot has a special characteristic of uninterrupted monitoring the behavior of the hacker/attacker and requires minimal resources to trace the movement. Honeyd is an open-source honeypot application that keeps virtual host on the network. It's a type of a low interaction honeypot which performs services like FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol). The greatest significance of the honeypot is its simplicity. It gives less or no traffic in the network. Whenever a connection is sent to the honeypot it is being accessed by unauthorized activity [11]. There are two different types of honeypot are as follows [8]: 1. Production Honeypot: - It's a type of low interaction honeypot, which is easy to use and has only inadequate information about

the hacker's reroute and justifying his attacks. It is applied in business corporations and organizations. 2. Research Honeypot: It provides detail information about the strategy and motives of the attacker [19]. There are different levels of Honeypot which can be categorized as:

- Low-interaction Honeypots: It requires only one physical machine. This honeypot gives information about the attacker who is frequently accessing the network. They use only a few resources on the multiple virtual machines with small reaction time. It requires less code by which the complexity of security gets reduced.
- Medium-interaction Honeypot: In this attacker is not in the statement with the real system. This honeypot did not give us specify information about the hacker. It provides incomplete service as compare to a low-interaction honeypot.
- High-interaction Honeypot: It works on an isolated network in which it hosts a variety of services. It gives the maximum amount of the attacker's information activities when interacting with our system. This technique is implementing on one physical machine per honeypot which directly increases the cost and maintenance.

Honeypot gives us valuable information about the attacker's action [9]. The honeypot is a system or computer who sacrifices themselves to target the attacks of hackers. Our main concern is to protect the data. So while designing the cloud it is necessary to implement such an authentication protocol which fulfill the needs of security and maintain the cloud storage.

Hence in this paper authors are tried to implement Kerberos authentication protocol for data security in the cloud. When Kerberos implemented on the network, increases the authenticity to secure the data of the client/host by a ticket or token granting ticket (TGT) [34]. It has time-bound and encrypts it by using the secret key in the ticket-granting service (TGS) [17].

II. METHOD

Nowadays, there is a bulk of data available which needs to be standardized, protected with their demand, Cloud computing is one of the best options for both data storage and security. So here an attempt is made to provide security to all the valuable data in the cloud network. This is made possible by implementing Honeypot cloud computing technique [25] and Kerberos authentication (developed for Project Athena at the Massachusetts Institute of Technology) [31] with AWS environment used as Platform as a service [26].

[1] Honeypot: It can control and grant security to the network activity like dropping of packets, system log files [12]. The conception of production honeypots is to copy real production systems, services, and some operating system to promote the hacker. They can also replicate different viruses and trojans to attract attackers. The use of high-interaction honeypot [15] minimizes the data loss in an organization. Security conventionally has been about the CIA (Confidentiality, Integrity, and Availability). It now also includes areas like Trustworthiness, Quality, and Privacy. Access control systems provide the essential services of identification and authentication (I&A), authorization, and accountability.

A high- interaction honeypot has a real underlying operating system. This guides to much higher risk as to the complexity increase quickly. At the same time, the potential to gather information, the possible attacks as well as the attractiveness increase a lot [22]. A high involvement honeypot does present such 24x7 an environment. As soon as a hacker has gained access, his real work and therefore the interesting part begins. Regrettably, the attacker has to compromise the system to get this level of freedom. An attacker will then have root rights on the system and can do everything at any moment on the compromised system. As per, this system is no longer secure. Even the whole machine cannot be considered as secure.

A high- interaction honeypot is very time-consuming. The system should be constantly under observation [22]. A honeypot which is not under control is not of much help and can even happen to danger itself. It is very important to limit a honeypot's access to the local intranet, as the honeypot can be used by the blackhats as if it was a real compromised system. Limiting outbound traffic is also an important point to consider. By providing a full operating

system to the attacker, he has the potential to upload and install new files. This is where a high-involvement honeypot can show its strength, as all actions can be recorded and analyzed.

[2] Kerberos: It is a computer network validation protocol to all major operating systems, such as Microsoft Windows, Apple OS X, FreeBSD and Linux that works based on tickets to allow users corresponding over an insecure network to confirm their identity to one another in a secure manner [10]. Kerberos protocol is as a default verification method in Windows. This name Kerberos [34] was taken from the Greek mythology "a three-headed dog" that guards the gates of Hades. These three heads represent a client, a server and a Key Distribution Centre (KDC). KDC [34] act as a third-party authentication service. By default, Kerberos uses UDP port 88. Kerberos model builds on symmetric key cryptography and needed trusted third party (KDC) which uses public-key cryptography. The three parts of the Kerberos are as follows:

1. Key Distribution Centre (KDC):- It holds all the information about clients and the secret key for the demanded service to authenticate the user. It is said to be a Domain Controller (DC) which is used to generate TGT [34] and SGT. TGT is a ticket-granting ticket which is generated for the client. It is responsible to issue a ticket for the user to obtain the service from the file server.
2. Client: - It's a user who is present in the network, to share the data. In the Kerberos model, only the user must be authenticated by generating the [34] TGT.
3. File Server: - Whomsoever the user in the network wants to share the data by taking permission from the server.

Functioning of the Kerberos model (shown in fig.1) in the network, as NTP (Network Time Protocol) is used to synchronize the time within the whole network [31]. (a.) Key Distribution Center (KDC) [34] which gets the request from the client then (b.) client gets the TGT from the KDC. When a client wants to send the data, in the network (c.) It sends request + TGT to the KDC. In reply (d.) KDC will send TGT with a timestamp to the client. (e.) The client sends the TGT [34] with a timestamp to the file server for the resources. (f.) NFS (Network file server) verify this client with the KDC. (g.) Verification gets successful. (h.) NFS then allow the resource which is to be shared by the client.

ISSN 2348 – 8034
Impact Factor- 5.070

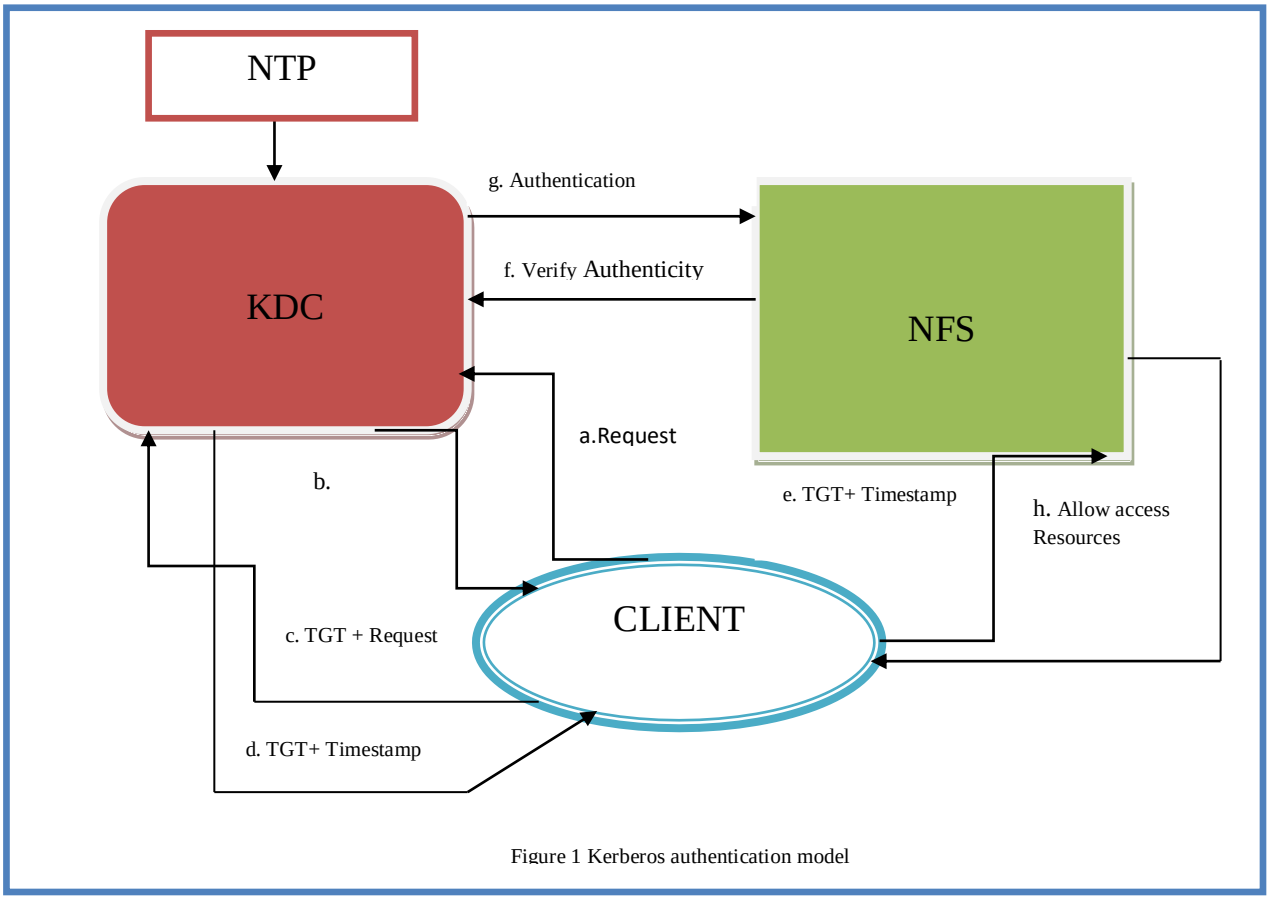


Figure 1 Kerberos authentication model

[3] AWS environment: Here in the AWS cloud environment using Kerberos and SELinux is installed in all the servers and clients of the network. Kerberos is giving security but using AWS cloud provider enhances the authentication through confidentiality, reliability, availability, and maintenance at a minimal cost [33]. Any hacker or attacker cannot fully access the system but hacking can be possible. Kerberos provides a solution to a security issue. Kerberos is installed in all the instances of AWS cloud surrounding and servers with SELinux. The SELinux (Security-Enhanced Linux) is a part of the Linux security kernel that acts as a shielding agent on servers. In the Linux kernel, SELinux relies on mandatory access controls (MAC) that restrict users to rules and policies set by the system administrator [32]. MAC is a higher level of access control than the standard flexible direct access control (DAC) and prevents security violates in the system by only processing necessary files that the administrator pre-approves.

III. RESULT AND DISCUSSION

The Kerberos authentication model helps in the development of a secure environment in cloud with AWS platform using honeypot. All the system connected with the router in the network and they all is connected with the firewall. High-interaction honeypot is connected with the internet and also to the firewall. If an attacker tries to enter in the system, high-interaction honeypot starts to monitor its activity. This whole process is automated to monitor and trap the intruder's activity. The attacker passes through the firewall enter into the instances of the cloud environment because of SELinux, it cannot access the instance and Kerberos checks the authentication and it will prove the hacker is a malicious user.

ISSN 2348 – 8034
Impact Factor- 5.070

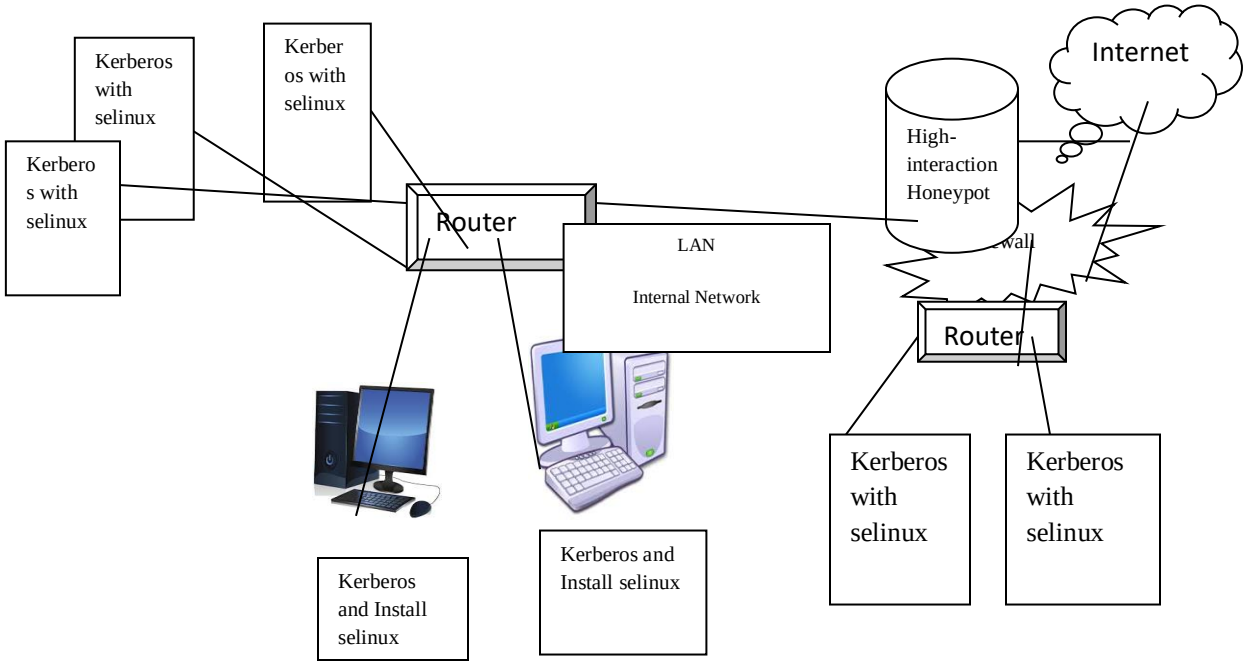


Figure2: The working of high-interaction honeypot, Kerberos, selinux in AWS cloud environment.

Figure 2 highlight the importance of honeypot in the Kerberos authentication protocol. As it is attached to all security providers. If any hacker or intruder tries to get enter in the network all its activity is recorded by continuous monitoring the system by using different protocols we implement the Kerberos in the AWS [30] cloud environment which is whole automated using Linux as an operating system. This Kerberos prevents the network by using Linux as very few know how to work on the CLI (Command Line Interface) [25]. Following steps are as follows:

- In Kerberos, TGT is generated with the use of encryption technique which implements symmetric key. After applying the decryption technique on TGT ticket with time stamp an asymmetric key is used [10].
- After the authentication of the client has been done successfully, then we get access permit in the network [32].
- If anyhow hacker tries to enter in the system through the biometric method then also it gets failed.
- If it gets fail then our network security controlling system will be crashed down and whole data saved in the server.
- In that case, the log file must be created as a report of any hacker and alarm must be generated through the mail to the authenticated user.

Here AWS cloud provider with [25] Kerberos5 (it's a version of Kerberos) with the three components like KDC, client, NTP (network time protocol) and file server is used. With the use of Kerberos in AWS environment it became more secure, cost-effective and ease in maintenance. In-network our file cannot be hacked by any malicious user. As steps of CLI Kerberos implemented in AWS cloud environment has shown in the following screenshots (from fig.3 to figure 9): fig.3 shows initialization of the Kerberos database with the password and its master key. Fig.4 shows the host which is created by adding princs command. Fig.5 KDC server which has the configuration of time-bound in which ticket has been generated. In this screenshot is defined the time-bound of a ticket which has 24 hours. Here in this fig.6 shows the NTP server created in which time is synchronized between host, KDC and server. Fig.7 shows the NFS client [30]. In this NFS serves the client, when it demands the resources and then it becomes the NFS client. In fig.8, NFS mount the client at the starting of the system when connectivity is established between them. In fig.9, the config of the NFS server and its connection with the KDC is shown.

[Saxena, 6(8): August 2019]
DOI- 10.5281/zenodo.3367428

ISSN 2348 – 8034
Impact Factor- 5.070

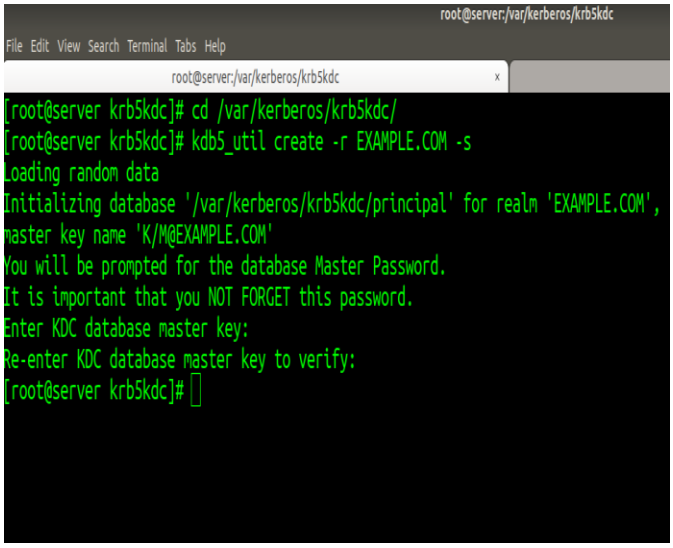


Figure3 It shows the Kerberos database

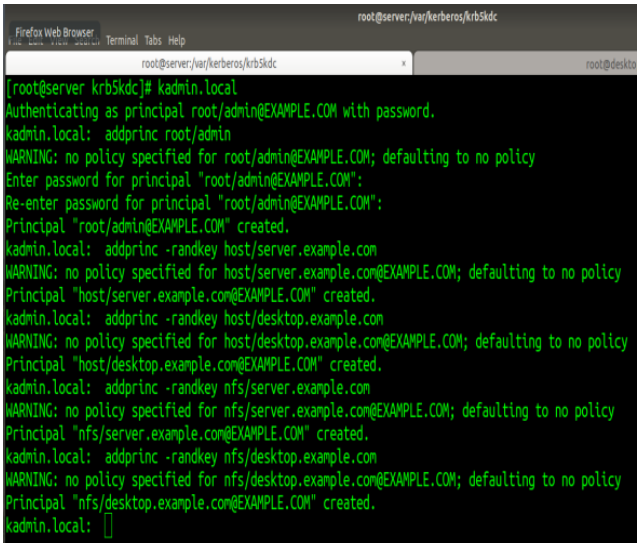


Figure4 shows the host/client of Kerberos

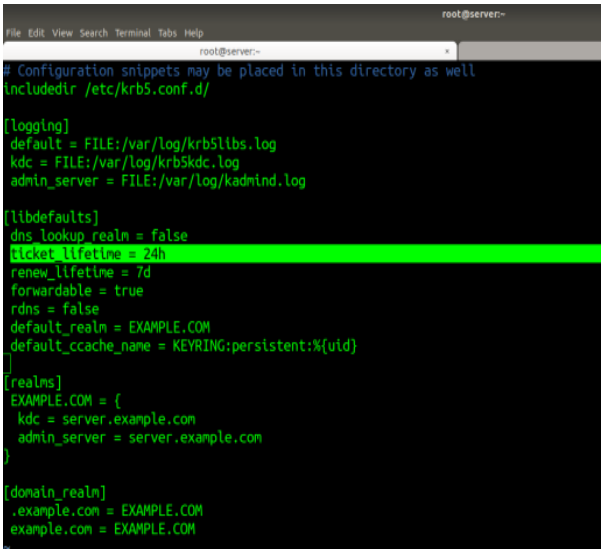


Figure 5 Kerberos Server Config

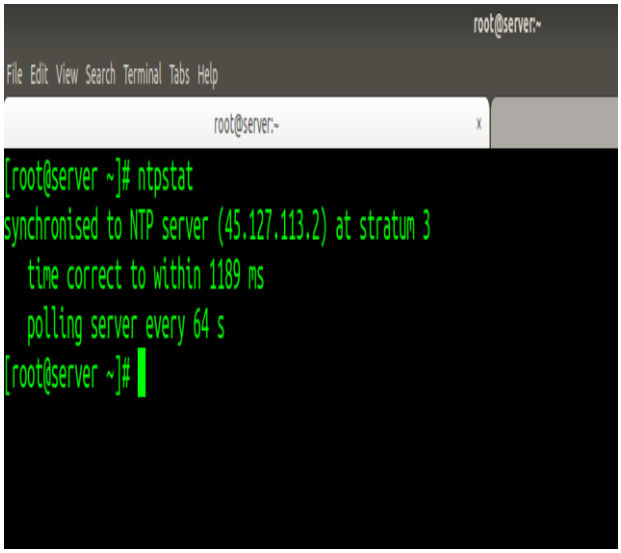


Figure 6 NTP Synchronization

ISSN 2348 – 8034
Impact Factor- 5.070

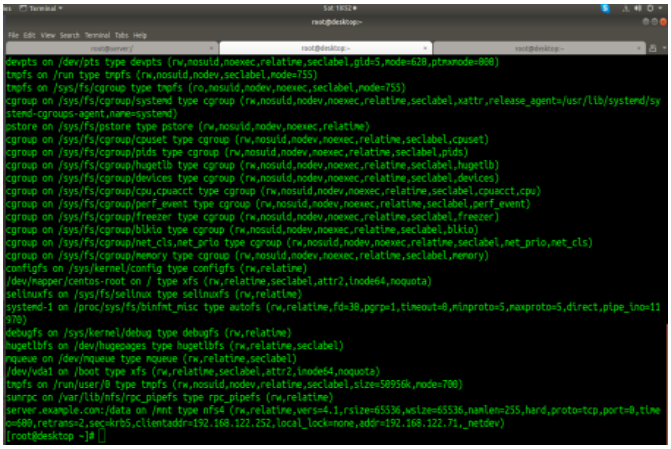


Figure7 Shows the NFS client

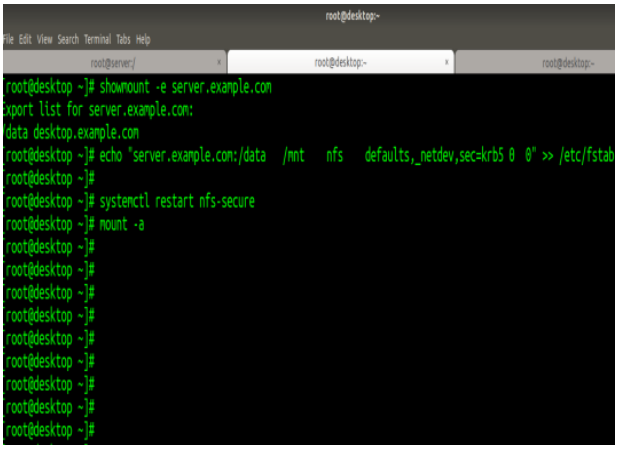


Figure 8 NFS mount the Client

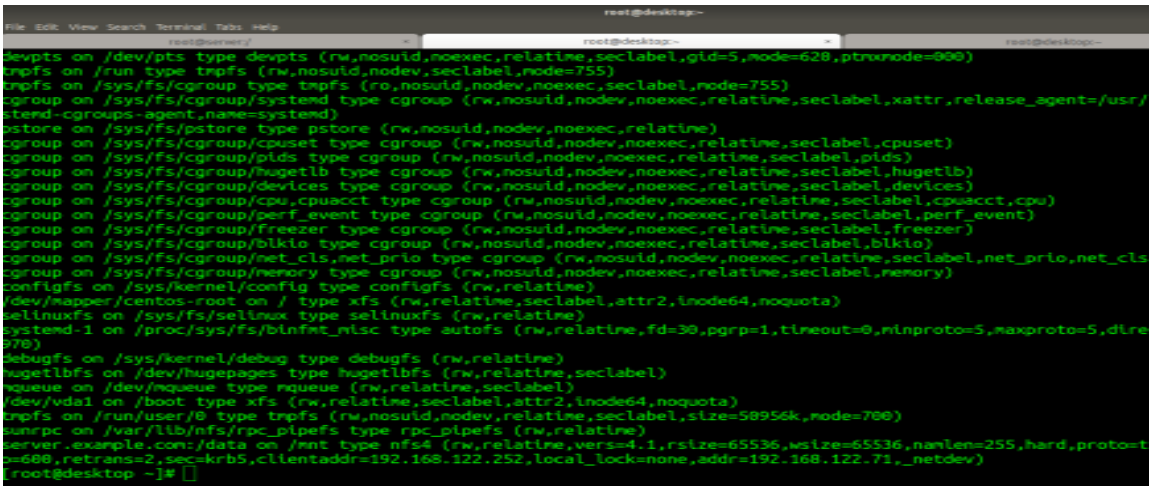
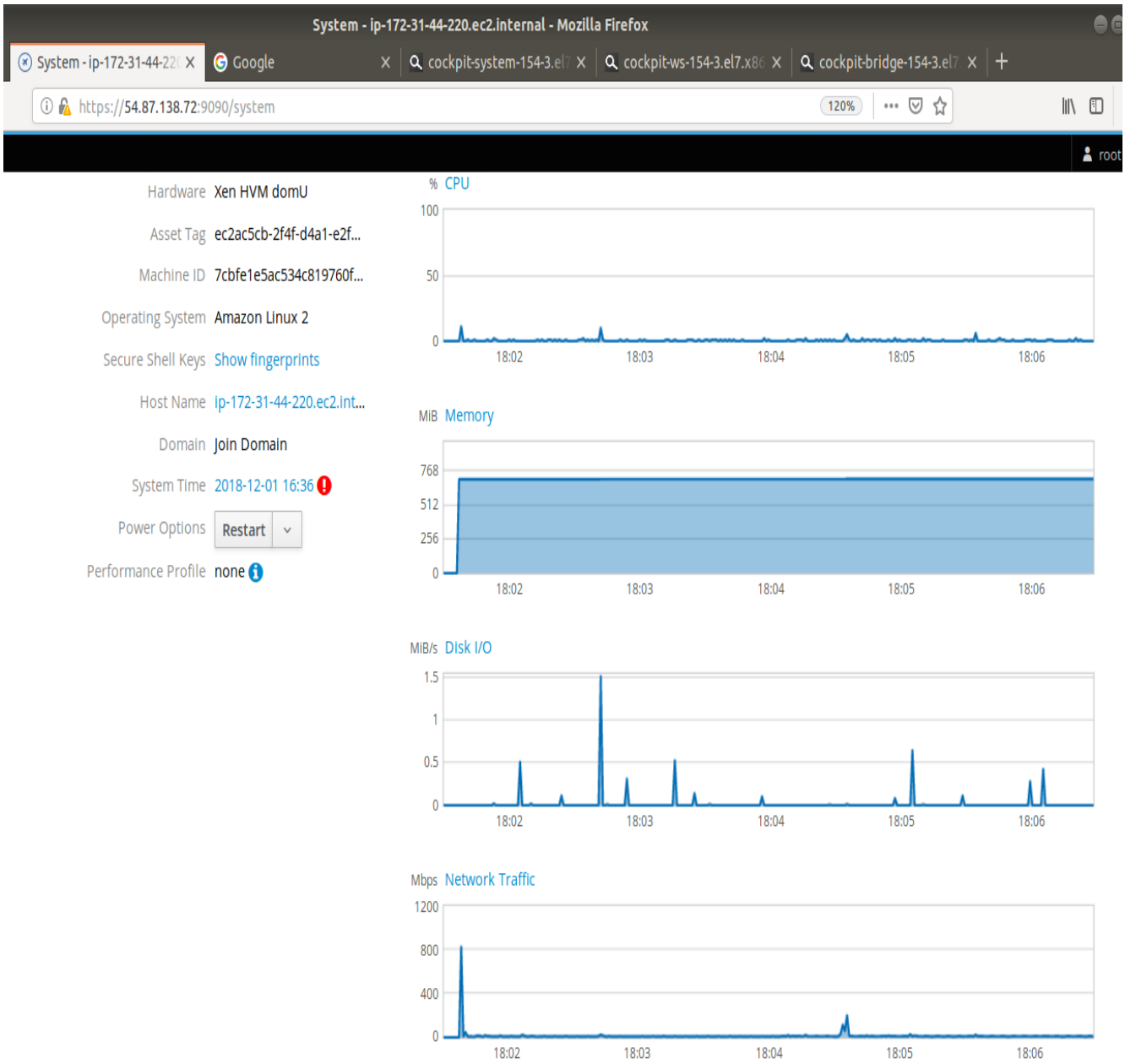


Figure 9. The NFS Server

In our proposed method, the verification between client and server is based on not only public-key cryptography but with a high-interaction honeypot technique. Nowadays Amazon Web Services (AWS) [30] started offering IT infrastructure services to companies in the form of web services normally known as cloud computing which is free to access to everyone after the simple registration process. One of the key benefits of cloud computing is the prospect to replace open capital infrastructure expenses with low changeable costs that will scale the business. Instead, they can immediately roll up hundreds or thousands of servers in minutes and deliver outcome faster. Amazon Web Services presents a highly reliable, scalable, low-cost infrastructure platform in the cloud that influences hundreds of thousands of businesses in 190 countries around the world.

With the use of high-interaction honeypot which is more complex and risk get higher for the unknown user. This AWS environment with Kerberos is liable to provide the service to the client in a structured manner and client uses those services to achieve the preferred task which is allocated exclusively for the user. An improvement of using client-server, it can attach isolated users with distant resources to match the authorization and verification phase of a protected distributed system. After using Kerberos an authentication protocol which gives our method more secure, reliable and maintains confidentiality, integrity, availability using AWS cloud in the network. These factors have been used for high-interaction honeypots, a log-file is generated on every activity of the intruder. It is a form of a

report of the malicious user. This gives the network more secure when any malicious progress happens. In graph1 it shows the status of the system after the creation of the instances through AWS Amazon cloud.



Graph 1. The working of the Kerberos in terms of system efficiency

According to graph1, it gives the specific detail of the information of the system like CPU, memory, disk I/O and network traffic. After the processing of the KDC, NTP, client and NFS server on the system it gives an overall effect of all these instances on the system efficiency and security of the data on the network with the honeypot technique.

- CPU shows the utilization of the system in a more efficient manner. Here on the x-axis is respect with time and y-axis is for percentage utilization of CPU.

- This linear graph in memory shows that it does not occupy any extra space whatever congestion is there in the network. On the x-axis is with respect with time and y-axis is for MB in size.
- These highest peaks in the disk I/O of the processor shows that this process of Kerberos with honeypot increases the efficiency of the system and network become more secure successfully. On the x-axis is with respect with time and y-axis is for MB/s (Megabytes per second) in size.
- In the network graph, it shows that some distant peaks make the network work efficiently in the presence of heavy traffic. On the x-axis is with respect with time and y-axis is for Mbps (Megabits per second) in size.

Our work is to implement Kerberos in AWS cloud provider with SELinux installed in the system give security more efficiently.

IV. CONCLUSION

As the present paper focused on to make the network more secure by the use of high-interaction honeypot with Kerberos5 and SELinux in the AWS cloud environment. Server-based security has been implemented in our proposed technique, honeypot with Kerberos. Soon, this can be implemented with the VPC (virtual private cloud) in the cloud environment through VPN (a virtual private network) to increase the system security, confidentiality, availability, and integrity. As it includes the feature of public cloud which permits organizations to speed up digital transformation with faster access to promising technologies such as artificial intelligence, big data analytics, the Internet of Things, block chain and cloud-native application development platforms. With the exactly public cloud platform, associations can be more cost-efficient, strategic and agile, without sacrificing project requirements for availability, reliability, security, disaster recovery or regulatory agreement.

REFERENCES

1. *G. E. Blonder: Graphical password, U.S.Patent 5 559 961, (1996).*
2. *R. Dhamija, A. Perrig, A user study using images for authentication. Proc. 9th USENIX Security Symp. CO, pp. 45– 58 Denver, (2000).*
3. *X. Suo, Y. Zhu, G. S. Owen, Graphical passwords: A survey, Proc. 21stAnnu.Comput. Security Appl. Conf, pp. 463–472 (2005).*
4. *Paul. A.J, Varghese Paul, P. Mythili: A Fast and Secure Encryption Algorithm For Message Communication, In IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), pp. 629-634 Chennai, Tamil Nadu, India. (2007).*
5. *Junjie Peng, et.al, Comparison of Several Cloud Computing Platforms In Second International Symposium on Information Science and Engineering 978-0-7695-3991-1 DOI 10.1109/ISISE. 94 23 (2009).*
6. *Joshi Ashay M., et.al, Enhancing Security in Cloud Computing. In: Information and Knowledge Management, Vol 1, No.1, (2011).*
7. *Ajeet Kumar G., et.al, An Improved Hybrid Intrusion Detection System in Cloud Computing. Int: International Journal of Computer Applications (0975 – 8887) Volume 53– No.6, (2012).*
8. *Stephen B., Rebecca L., Shishir P., Sivasubramanian R., and Josh S., Honeypots in the Cloud University of Wisconsin – Madison, December 19, (2012).*
9. *Nithin C., S.R, Madhuri, Cloud Security using Honeypot Systems, In International Journal of Scientific & Engineering Research Volume 3, Issue 3, (2012).*
10. *Aishwarya.S, et.al, Implementation of Honeypot using Kerberos Authentication In International Journal of Computational Engineering Research (IJCER), (2012).*
11. *Michael Beham, et.al, Intrusion detection and Honey pots in nested virtualization environments In DSN, 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp1-6 Budapest (2013).*
12. *Hwan-Seok Y. , A study on attack information collection using virtualization technology,74:8791–8799, Springer Science + Business Media New York (2013).*
13. *Al Awadhi, E, et.al, Assessing the security of the cloud environment, In IEEE Conference, Page(s) 251 – 256 (2013).*
14. *Kumar S., et.al, A Prevention of DDoS Attacks in Cloud Using Honeypot In International Journal of Science and Research (IJSR) Volume 3 Issue11 (2014).*

15. *Muhammet Baykara, et.al, A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems, Int: International Journal of Computer Networks and Applications (IJCNA) Volume 2, Issue 5 (2015).*
16. *Ramya.R: Securing the system using honeypot in a cloud computing environment, Int: International Journal of Multidisciplinary Research and Development, Volume: 2, Issue: 4, 172-176 (2015).*
17. *Hoa Quoc Le, et.al, A New Pre-authentication Protocol in Kerberos 5: Biometric Authentication Conference Paper, DOI: 10.1109/RIVF(2015).*
18. *Romendrapal Singh Rathore, et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, pg. 120-127(2015).*
19. *Marcin N., et.al, A Survey on Honeypot Software and Data Analysis arXiv:1608.06249 Cryptography and Security (cs.CR);(2016).*
20. *Sultan A., et.al, Data Security, Privacy, Availability, and Integrity in Cloud Computing: Issues and Current Solutions Int: International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 7, No. 4, (2016).*
21. *Gagan, Dr. C. Rama K., Rohit H., Dynamic Cluster-based Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data 978-1-4673-8203-8/16/ 2016 IEEE Int: 6th International Conference - Cloud System and Big Data Engineering (Confluence) (2016).*
22. *Akshay A. Somwanshi, et.al, Implementation of Honeypots for Server Security In International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 03 (2016).*
23. *Yunfei CI, et.al: Design and Implementation of the Components of the Symmetric Cryptographic Algorithm" Int: IEEE Second International Conference on Data Science in Cyberspace 978-1-5386-1600-0/17 IEEE DOI 10.1109/DSC.2017.23 (2017).*
24. *Liangxuan Zhang, et.al, Privacy-Preserving Attribute-Based Encryption Supporting Expressive Access Structures Int: IEEE Second International Conference on Data Science in Cyberspace 978-1-5386-1600-0/17 IEEE DOI 10.1109/DSC.2017.61 (2017).*
25. *Ashok Kumar J, et.al, A Modified Approach for Kerberos Authentication Protocol with Secret Image by using Visual Cryptography In International Journal of Applied Engineering Research Volume 12, Number 21 pp. 11218-11223 (2017).*
26. *AZURE Homepage, https://azure.microsoft.com/en-in/overview/what-is-cloud-computing,last accessed 2018 /09/27.*
27. *Chaimae S., Habiba C.: Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb, Int: International Conference on Computational Modeling and Security (CMS 2016), Morocco (2016).*
28. *Sushant M., Makarand K., Krantee J.: Application of Honeypot in Cloud Security: A Review, Int: International Journal on Future Revolution in Computer Science & Communication Engineering (2018).*
29. *Nooreen Fatima Khan, et.al, HONEY POT AS A SERVICE IN CLOUD In International Journal of Pure and Applied Mathematics Volume 118 No. 20 (2018).*
30. *AMAZON Homepage, https://aws.amazon.com/about-aws/, last accessed 2018/11/25.*
31. *Kerberos, https://cbt.gg/2CsnIRh,last accessed 2018/11/01.*
32. *https://searchdatacenter.techtarget.com/definition/SELinux-Security-Enhanced-Linux*
33. *https://www.youtube.com/watch?v=FBnTeryebzc*
34. *Megha Singh, et.al, MULTI SECURITY SYSTEM BASED ON HONEYPOT USING KERBEROS ALGORITHM, International Journal of Modern Trends in Engineering and Research (IJMTER) Volume 05, Issue 2, 2349–9745(2018)*
35. *Apurva Saxena, et.al, 2018 "Honeypot based new algorithm for data security" Journal of Engineering Research and Application Vol.8, Dec.*