International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 6 Issue 6 June 2019
ISSN Online: (2455-4723)

Kerberos based Enhanced Authentication Protocol for Cloud Computing Environment

Aaradhana Sonakiya Student BM college of technology Indore, M.P. aaradhanasonakiya@gmail.com	Mohit Jain Assistant Professor BM College of Technology and Science Indore, M.P. bmctmohitcs@gmail.com

Abstract

Cloud Computing is one of the most famous field in the world of computer science research. The layered architecture forms a pyramid with categorization SaaS, PaaS&IaaS laid top to bottom. The user of this service model goes pay-per-use basis to the service provider. Like the other popular field, cloud computing too attracts those who likes to find loopholes to benefit themselves illegally. In this paper, we are using Kerberos at the server end, to avoid third-party dependency. To achieve confidentiality, cryptography is also taken in use along with the elliptic curve.

Keywords— *Cryptography; Security; ECC; Kerberos; Cloud Computing*

1. INTRODUCTION

Cloud computing is been known and applied on a huge scale in any business organization. The ease of access to the services is the primary reason behind the popularity of cloud computing. In this model, software, platform, and even entire infrastructure is capable of getting delivered to all possible ends. Cloud computing bags all the leading organizations as it's investor & they provide the ease of access on pay-per-use basis. To expand business and gain popularity, some new cloud vendors are providing free services too. Windows Azure, Google Drive, Apache Hadoop are some famous examples of cloud vendors. Cloud computing is both efficient & scalable service, it lowers down the memory requirement & computation time too.

With all the ease of access and enabling users to enjoy services from all possible ends of the world, Cloud computing surely lacks when it comes to security. Processing cost and computation is compromised while providing the required security, hence most of the time security stays as a compromised entity. Encryption is used in security but that is just a part of it and never fulfil the requirement. Security feature is claimed to be provided by all the leading cloud vendors. To achieve a user compatible atmosphere, security is a must factor.

Cloud designer distributed the model in different parts to make every user compatible with it, let the user be an employee, home based user, or CEO of an organization. The sub-units are categorized as under:

Private Cloud: An architecture designed and framed to provide service to a specific company or organization, where no other from outside is allowed to enjoy the services, is referred a Private Cloud.

Public Cloud: An architecture framed to provide the services to everyone with complete access is called a Public Cloud.

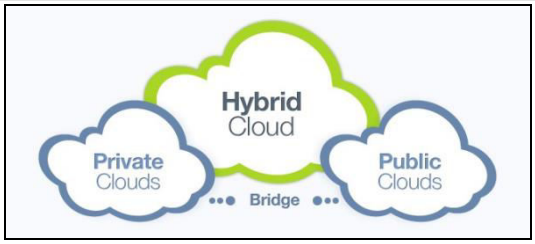

Fig. 1: Cloud Environment

Hybrid Cloud: It is a fusion of both private & public cloud. Hybrid Cloud distributed the workload between both public & private organizations as per the requirement.

Below is the detailed categorization of the services, which are achieved by portioning the cloud further:

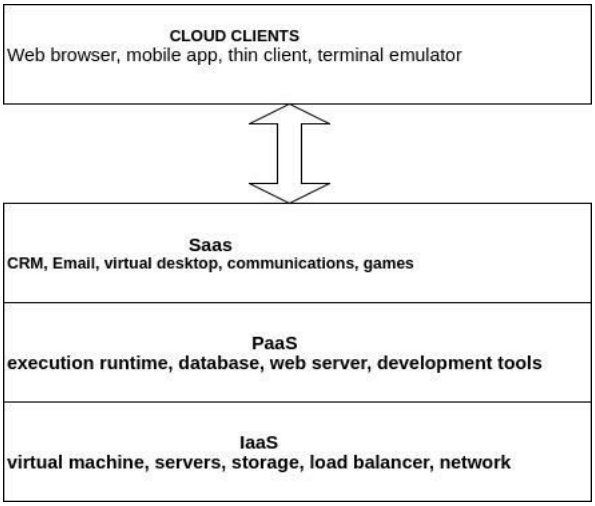

Fig. 2: Cloud Service Architecture

Infrastructure as a Service (IaaS): It is also known as utility computing. Integral software, web-based services & all other utilities like storage is offered in Infrastructure-as-a-service by the cloud vendor. Best known example is "Azure Web Services". The operator provides a system achieved by the merger of networking, processing & storing, this system is capable enough to work as a platform and as a software for the user. IaaS is best represented by virtual machines.

Platform as a Service (PaaS): In this form of cloud service, the cloud vendor allows the user to access operating system utilities but not all the services, then it becomes a Platform-as-a-Service. PaaS is best explained with example, Postman.

Software as a Service (SaaS): When a software is offered by the cloud vendor to the users, against of their service fees paid by the user, then this system is called as Software-as-a-service. SaaS is best explained with example, Email.

Internet is the basic demand to make the whole cloud architecture work. It is very important to have a communicable environment, as the services are rendering. All big enterprises already have huge amount of resources and as cloud market is known to everyone out there, this creates a demand for the enterprises to invest in this field. Cloud is available for any requirement, let it be building a website or hosting one, this also allows to provide the facility of consuming.

Cloud security is an interesting area of research as achieving the best security will definitely open new possibilities in future. Different encryptions & access control policies are developed to bring out the best possible security in the system. If we take Hadoop as our example, they use key factors like HDFS, map reduce for security purposes. According to the system requirement, encryption & other security schemes can be applied as well.

Whenever information technology security is been discussed, it is required to cover the drawbacks too, in order to make it foolproof. Processing time, memory consumption, computation overhead and others can be calculated as the drawback examples.

Despite having many techniques available in today's scenario but still applying them all isn't possible as it will shoot the computation cost very high. Memory

requirement at the server end will turn so high that the whole system will lose its applicability for most of the users.

As the requirement of Cloud services is increasing, the need of security is also spreading vastly, it consists of many encryption techniques. It is important to have security as intruders are always ready to steal important data. Enhancement of processing time, computation and bandwidth are bagged too in the list of benefits of security. Best example for cloud service is Google, which provides all its homegrown app to the users.

A wide range of business & services enjoys the application of Cloud computing. Let it be a hospital, which uses cloud computing to reserve and access past history of their patients or a vehicle assembly unit, which uses it to arrange the right part according to the assembly plan. Maintenance of all the services is the job of cloud provider. Thanks to cloud computing, now we do not need to buy and install expensive software in our computers, we can access them via cloud. Amazon web services is the best example to explain this thing, as you can get a perfect environment for web development via AWS.

2. LITERATURE REVIEW

MrudulaSarvabhatla et al. In [1] to save user from cyber-attack, they present a planned authentication system. This system decreases both overload & resource consumption. It uses XOR operations which is less expensive than others, also this strategy uses 3 steps: Login, Registration & Mutual Authentication.

Head et al. [2] developed a model called Virtual Hypervisor, which has a potential to provide much better control over resource allocation.

Jung et al. [3] to allocate the desired data, they proposed a resource allocation model. Proper data center & workload on each data center are the 2 main measurements on which the whole agent-based model runs.

TumpeMoyo et al. [4] developed an E learning tool. A close observation is made about open cloud environment & compared with private cloud in this work.

Chen, D et al. [5] talks about the importance of security in cloud computing. Services are made accessible via cloud by the service provider to make the user comfortable while working, but at the same time secured architecture is a major concern too. Hadoop ecosystem uses Airwet to secure the system and is made to work along with Map reduction framework to bring out the best results.

Emeakaroha et al. [6] presents a resource manager environment of dynamic virtual allocation. This whole environment consisted 3 main components and those are: Resource Manager (RM), Subscribe Server (SS), and User Interface (UI). By the providing the correct username & password, the user is authorized to access the cloud. Resource Manager is designed to take care of the other 2 components, it pushes the subscription message to Subscribe Server & accepts the virtual machine request from the User Interface.

K. Nasin, et al. In [7] focuses on how cloud can serve the research for information technology better. A fusion of RSA & AES is applied to achieve better security. This combination makes it really difficult for the intruders to find loopholes and fail the system at any point.

Cindhamani Jet et al. In [8] used RSA & third-party auditor. To create an efficient security architecture, 128-bit key are taken in use. An advanced form of authentication

service is used in this work to achieve reduced overhead & enhanced refinement.

Jayant.D et al. In [9] in their work infused RBAC with the encrypted text coming from the combination of RSA & AES, this whole provides a seamless security feature known as access control.

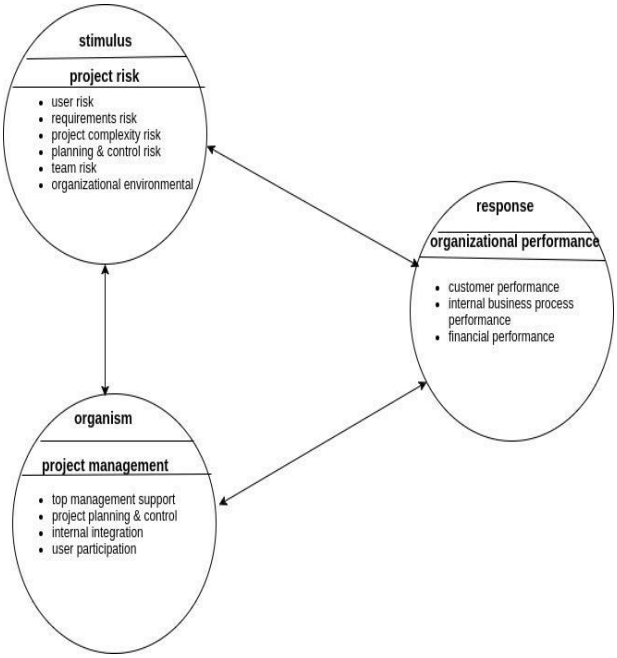

Fig. 3: Cloud Authentication Scheme

Yazir et al. [10] states about the dynamic resource-based approach. A distributed network of NAs is designed by them, which holds to potential to handle management of the system. Awareness in resource availability & global approach is taken care in this network maintenance system.

3. Kerberos Authentication Scheme

Kerberos is capable of providing authentication to the system & also pretty famous security protocol. It is applicable in both centralized architecture and distributed architecture, but it is developed to mainly deal with distributed environment. A long-term secret key is first created by the user, this password will be asked by the system whenever the user demands service. TGT is Ticket Granting Ticket, and every user has it already. TGT is designed to use n multiple servers as it is used to verify the client. Now, when TGT is received from the server end, the client demands for service granting ticket, so that the user can proceed with the services provided. The Authentication Server AS is responsible to verify and provide entry ticket to the user and TGS is responsible to allocate the service grating ticket to the user. A combination of Database, Ticket Granting Server & Authentication Server forms a key distribution center.

Kerberos follows the below written steps for authentication:

a. A request for granting ticket is made to authentication server, right after a logging in process is performed on workstation.
b. The data entered by the user gets checked by the authentication server and if the input matches the records, it assigns TGT and a session to the user. The user can communicate with the server in the given session time.
c. The ticket that Authentication Server issues to the client includes the same copy session key.
d. The server and client, both keeps the key.

Later, using the password of the user, both session key & TGT is encrypted. There is no chance that any user can achieve the access of the other user as the encryption has the user specific password in it. Also, both the server & client has the password, this even lower down the chances of wrong access.

Limitations

1. The whole operation is performed under an untrusted network and this allows the possibility too that the host itself is untrusted.
2. Relocation of password to some other place will be totally unsecured in Kerberos
3. A source should be available to make calls like the compulsion of using the local libraries in order to use Kerberos.
4. Unencrypted transfer of password is never allowed on Kerberos but if you still do that, Kerberos consider this operation at your own risk.

4. PROBLEM STATEMENT

Cloud computing comes in the list of most used network in today's world, some use it for services while others use it for platform. In this system, the whole server is set-up at some other location, while the users are spread across every corner. The cloud providers gives the access of services to the user but lacks when it comes to security. A mechanism is the need of the hour for both the user and the cloud server. The security must provide features like encryption, non-integrity, availability & authentication.

Authentication is such mechanism that makes sure that the request is made by the correct user and not from some intruder. In this system, if the user side fails to satisfy the server, then no third-party can intrude and get the access at any point. Weak authentication is never a security factor, and having no proper security calls for high risk for the user. As the risk increases, security threats shoot up as well. The researches kept this in mind and other security protocols too, hence strong authentication is recommended for the security of the account.

Including integrity & other several security mechanisms, there are many mechanisms applied in the system. Certain techniques like password-based security is introduced but passwords are trackable. A variety of security like third-party security, social security and others are involved in Authentication Mechanism.

Our works suggests that Kerberos provides the required security successfully to the system & the paper demands to include Kerberos in Cloud Computing.

5. SOLUTION DOMAIN

The need of security is very strong for both the user and the server. A best authentication system with strong cloud computing policy should be presented. In our solution, a better authentication system than username & password is achieved by using Kerberos as authentication scheme. A hybrid security is applied in our approach, KDS have both TGS (Ticket Granting System) & Authentication Server (AS).

The scheme created in our work should provide better security to have authentication. A proper secure communication between the cloud user and server is a must in all cloud-based models. The architecture should have brilliant access control. Unique access structure is designed with homomorphic encryption.

By avoiding the security breach of authentication, we can overcome data isolation issues in our work.

Our work is accessible for multiple providers and analyses the resources better. We took security one step ahead by using TGS & AGS, which eventually provides features like accountability. The access grand and refrain access is kept on the user end, hence our solution is much better than simple authentication.

A block diagram to represent the same is shown in Figure 1.

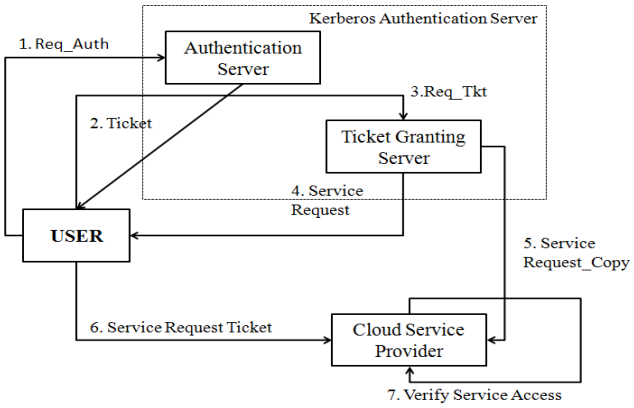

Fig. 4 System Architecture

6. CONCLUSION

As we are well-known to the fact already that security is the basic need of the cloud system. The work discusses here the application of Kerberos which provides seamless security. Merging ticket granting approach with Kerberos can achieve desired security. Kerberos security in cloud-based architecture is suggested in our work paper. Calculation of computation time & other factors including implementation of the given solution can be a given in the future work on this paper.

REFERENCES

1. MrudulaSarvabhatla, Chandra Mouli Reddy M, Chandra SekharVorugunti, "A Secure and Light Weight Authentication Service in Hadoop using One Time Pad", "2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)", Procedia Computer Science 50 (2015) 81 – 86.
2. M. R. Head, A. Kochut, C. schulz, and H. Shaikh, "Virtual Hypervisor : Enabling Fair and Economical Resource Partitioning in Cloud Environment", in IEEE Network Operations and Management Symposium (NOMS'10), Osaka, 2010,pp. 104-111.
3. G. Jung, and K. M. Sim, "Agent-based Adaptive Resource Allocation on the Cloud Computing Environment", in 40th International Conference on Parallel Processing Workshop (ICPPW'11), Taipei City, 2011, pp. 345-351.
4. TumpeMoyo, and JagdevBhogal, Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems, 2014.
5. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", "International Conference on Computer Science and Electronics Engineering", 2012.
6. V. C. Emeakaroha, I. Brabdic, M. Maurer, and I. Breskivic, "SLA-Aware Application Deployment and Resource Allocation in clouds", in 35th IEEE Annual Computer Software and Application Conference Workshops, Munich,2011,pp.298-303.
7. NasrinKhanezaei, ZurinaMohdHanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", "System, Process and Control (ICSPC), 2014.
8. Cindhamani, NaguboyniaPunya, RashaEalaruvi, L.D. Dhineshbabu, "An enhanced data security and trust management enabled framework for cloud computing systems", Computing, Communication and Networking Technhologies(ICCCNT), 2014.
9. Vishwanath s Mahalle, Aniket K Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm", "Power, Automation and communication (INAP)", 2014.
10. Y. O. Yazir, C. Matthews,R. Farahbod, S. Neville, A. Guitouni, S. Ganti, and Y. Coady, "Dynamic Resource Allocation in Computing Clouds using Distributed Multiple Criteria Decision Analysis", in IEEE 3rd International Conference on Cloud Computing(CLOUD'10), Miami,FL,2010,pp.91-98.