International Journal of Theoretical & Applied Sciences, 9(2): 25-30(2017)

ISSN No. (Print): 0975-1718
ISSN No. (Online): 2249-3247

Kerberos based Enhanced Authentication Protocol for Cloud Computing Environment

Sweta Jain* and Dr Vineet Richhariya**
**M. Tech. Scholar, Department of Computer Science & Engineering,*
Lakshmi Narain College of Technology, Bhopal, (Madhya Pradesh), India
***HOD, Department of Computer Science & Engineering,*
Lakshmi Narain College of Technology, Bhopal, (Madhya Pradesh), India

(Corresponding author: Sweta Jain)
(Received 22 July, 2017 accepted 12 August, 2017)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: One of the very well-known field in research of computer science result in the name called as cloud computing. The design is in the form of layered architecture with categorization as IaaS, PaaS and SaaS. The model provides the services to service providers in return of pay per use basis. Any field with popularity leads to inventors which find loopholes in the system to misuse it. In our work the third-party dependency is removed using Kerberos applied at server end. Along with it the elliptic curve cryptography is also used in order to achieve confidentiality.

Keywords: Security; Kerberos; ECC; Cloud Computing; cryptography

I. INTRODUCTION

Cloud computing is one of the widely known and adapted field in any business organization. The reason behind the popularity of cloud computing is easy to access services. All the possible ends whether the platform, software or even entire infrastructure in cloud is capable of delivering services with ease. All the leading organization are investors of it and providing easy to use services on pay per use basis. Some new cloud vendors are providing more services for free in order to increase there business and popular there companies. Examples of some cloud vendors are Google Drive, Apache Hadoop, Windows Azure and many more. The best part of cloud is, its efficient as well as scalable service. The computation time and memory requirement decreases in very well amount due to this services.

Cloud computing enables users to have services from all possible ends but the major concern which most of them lacks or not achieve efficiently it is security need. The security always comes with compromise in computation and processing cost hence most of the time it is compromised. The security is often concept with the encryption though encryption is just one aspect of the security. The entire leading cloud vendor provides the entire security feature somehow. Security is desired in order to have user compatible atmosphere.

In order to make every user compatible, whether user is an employee or home based or CEO of any organization, cloud designer partitioned the deployment model in several parts. The cloud based model is famous because of it. The categorization of subunits is mentioned below:

Private cloud: The architecture which is solely framed from specific organization and no outsider will be allow to access is called as private cloud.

Public cloud: The architecture which allow outside complete access with no chaining is refereed as Public cloud.

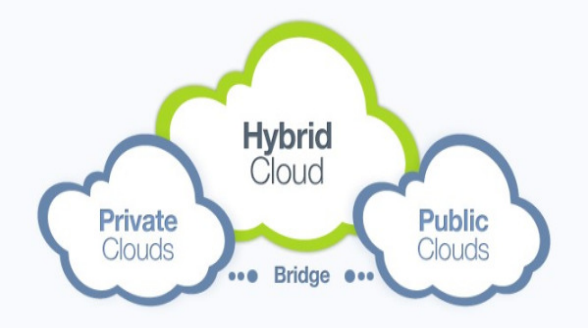

Fig. 1. Cloud Environment.

Hybrid cloud: It is the aggregation of public and private cloud. It uses the services of both public and private cloud by distributing the work load between both as the requirement.Separated from this, cloud is also partitioned in some other forms called services. The detailed categorization of it is given in Fig. 2.

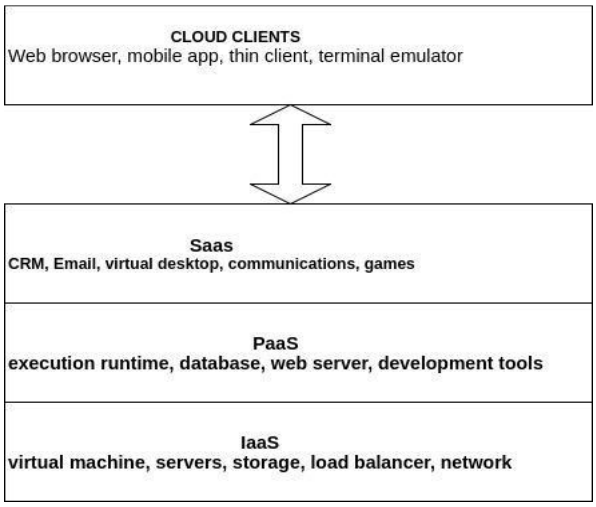

Fig. 2. Cloud Service Architecture.

Infrastructure as a Service (IaaS) : Infrastructure-as-a-Service is the level in which integral software , web services and all other utilities such like storage is offered by cloud vendor. The instance of this is Azure web services. It is also titled as utility computing. Networking, processing, storing all are merged to have this as service. It is put-upon by operators which are providing the left over two services which are platform as well as software. Virtual machines are best representative of IaaS.

Platform as a Service (PaaS): Platform as a service is outlined as when cloud vendor request operating system utilities but not all the services then it is called as platform as a service. Postman is the best example for PaaS.

Software as a Service (SaaS) : Software as a service can be outlined as services in which software's are offered by cloud vendors and certain sum of money for that software is payable to user. Email can be example of SaaS.

The central demand in cloud architecture is existence of Internet. As the extrinsic service provider is rendering the services, it must have some environment through which it can communicate with user. All the ample enterprises are financing in it as the resource are available in them in huge amount and market of the cloud is known to everybody. No matter what the requirement is whether it is hosting an website or building one such cloud is available. It is also available to provide the facility of consuming.

Cloud security is very well-known and interesting area for researching in order to explore the possibilities in current scenario. Various encryption techniques are developed as well as access control policies in order to provide best possible security. The architecture realizes the importance say for example if we are taking the example of Hadoop then various key factors like map reduce, HDFS in present in it. The encryption and other security schemes can be applied anywhere based on the requirement of system.

Whenever in any field of information technology security is discussed it drawbacks are also considered. The drawback examples can be calculated in terms of computation overhead, processing time, memory consumption an many other.

Though there are many techniques available all can't be apply as the computation cost which will be result can be eye opening. The memory requirement at server end will be so high then it will make our system poor in applicability.

Cloud security increases its arena so vast that it consists of so many encryption techniques examples of this are attribute based encryption. The need of security is must as the system intruders can lead to important resource losing. Cloud security also leads to enhancement of bandwidth, processing time and computation. Cloud security desired to have the model which is user need at a time. Cloud best example can be viewed as Google which provides all the apps. The infrastructure based service is desired when all the services from cloud are used whereas software based service is used when software's are needed.

Cloud computing has become the part of all the wide range applications. All the large enterprises are using it in wide scale examples of this can be hospitals are using the clouds services to access the past history of patient whereas vehicles are using it for assembling all the desired parts.

Cloud providers are responsible for maintaining all the services. Any software which we need in day to day life doesn't require to be downloaded instead it can be used via cloud services. One of the very well-known cloud service is Amazon web services which is used to provide the entire web development environment.

II. LITERATURE REVIEW

Chen, D *et al.* (2012) discussed the significance of security in cloud computing. Services provider are providing the facility of accessing the services using cloud, in order to makes user compatible in working, the need of user is to have secured architecture. Airwet is opted in order to provide security in the system, the Hadoop ecosystem is analyzed in the work and Map reduce framework is implemented along with [1].

Tumpe Moyo *et al.* (2014) developed an E learning tool. In this work, the importance of open cloud environment is observed and compared with private clouds [2].

K. Nasin, *et al.* (2014) described the significance of cloud in research in field of information technology. AES and RSA are implemented together in order to have more security. The benefits of both are considered. As the intruders are always focusing in finding attack the aim of work is to make vulnerability breaking difficult [3].

in his work, the combination of RSA and AES are used to have encrypted text along with it RBAC are used in order to achieve security feature called as access control (Jayant *et al.* 2014) [4].

Cindhamani Jet *et al.* (2014) 128 bit key is used in it for more efficient security architecture. RSA and third-party auditor is also used in it. Authentication service is implementing in this work with more refinement and reduces overhead [5].

Mrudula Sarvabhatla *et al*. (2015) present a built authentication scheme in order to prevent user from attacks. Planned authentication scheme have resource reduces resource consumption along with decrease of overload. This strategy uses three steps registration, login, mutual authentication and used less expensive approaches utilizing XOR operations [6].

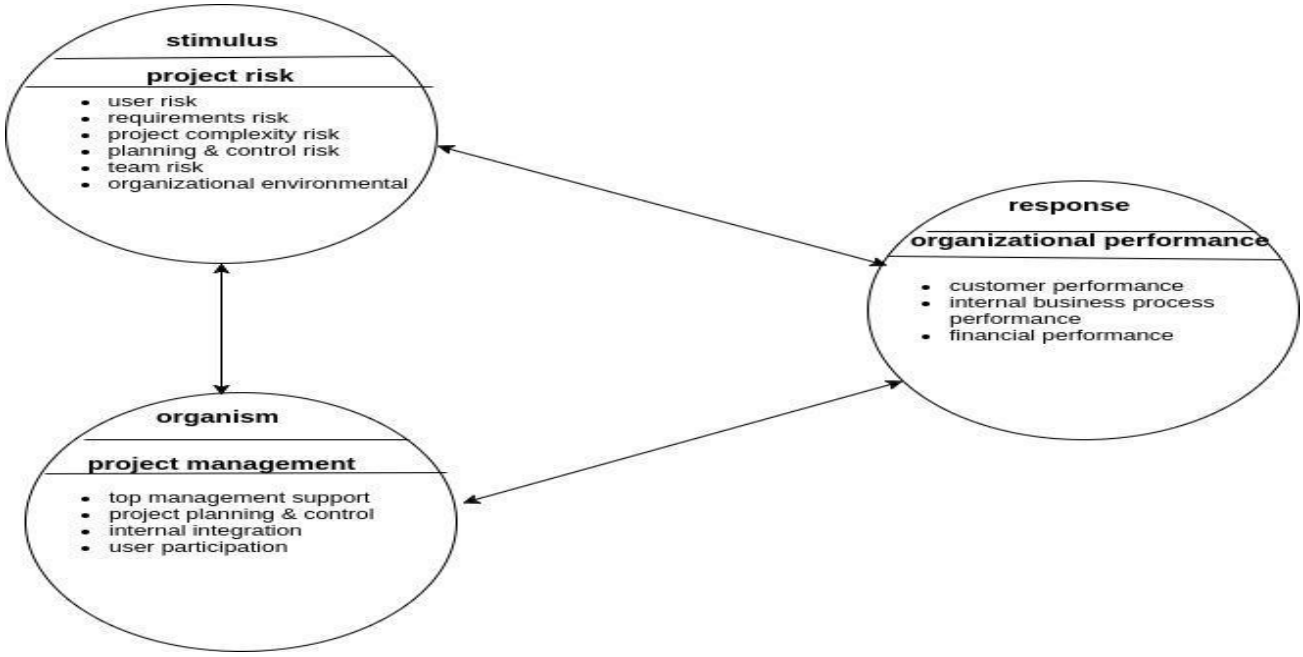

Fig. 3. Cloud Authentication Scheme.

Jung *et al.* (2011) proposed about the resource allocation model to allocate the suitable data. He implemented the model as an agent based, which is based on two measurement, first is proper data center and second one is the workload on each data center.

Yazir*et al.* (2010) defined the approach based on dynamic resource. He designed the system as a distributed network of NAS which is capable in handling the management. The network maintained in it is for the awareness in global approaches and resources availability [8]. Emeakaroha *et al.* (2011) introduces a resource manager environment of dynamic virtual allocation for cloud computing.

He also describe about the three components which are: User interface (UI), Subscribe server (SS), and Resource manager (RM). User has authority to access the cloud with providing correct user name and password. Resource manager works as it accepts the virtual machine request from user interface and subscription message to subscribe server [9].

Head *et al.* (2010) designed a model for powerful solution manager to have better control over resource allocation, the model named as Virtual Hypervisor model [10]. The work is simulated using CloudSim based tool. The results are significant in terms of Cost (profit) and Cloudlet execution [11]. Javed Akhtar Khan and M.R. Alony, (2015) introduce mobile SMS based blood bank management system for rural area which is direct connect to cloud server located in other location. Because in rural area blood bank management system not have a sufficient facilities for storing a blood in long time [12]. The main goal of this research is to provide techniques for solving problems of data security and load balancing related issues [13]. Thakur and Awasthi explore an expounded investigation of IaaS parts' security and decides vulnerabilities and countermeasures [14]. Cloud Computing is the technique in which virtual resources and services are offered to the user through the internet [15].

III. KERBEROS AUTHENTICATION SCHEME

One of the well-known security protocol which will provide authentication is Kerberos. It can be used in distributed architecture as well as in centralized architecture. But it is design for distributed environment mainly. Initially the password is created by user which is called as long term secret key. Each client will have TGT which is commonly known as ticket granting ticket from authentication server (AS). This TGT can be used in multiple servers as this TGT will be used to verify client. Once the TGT is received from server then the client demands for Service granting ticket. The database stores the assigned entities of user.

Whenever we want to access any data the Service-granting -ticket will demand the password every time. The key distribution center is collection of authentication server, ticket granting server and database. The AS is responsible for ticket granting to all the user and TGS is responsible for Service granting ticket to user.

The authentication can be perform in following steps in Kerberos:

a. Initial logging is perform in the workstation, the message is send to authentication server for request of granting ticket.

b. The checking in authentication server is performed, which check the data being feed by the user. If data input is correct then it assign TGT to user and also a session of user is also decide using key. In that session time the user can communicate to server.

c. Same copy of session key is also included in the ticket that AU issues to the client.

d. The key is kept by both which is client and server both.

2. Both TGT and session key is then encrypted using password of the user. As the encryption is performed using the key of user there are no chances that any other person can access it. As the key is known to both nobody else can access it.

Limitations

1. In an untrusted network entire operation is performed hence using an untrusted host the operation is performed it may be possible that the host itself is untrusted.
2. The password if relocated in some other place will be dangerous in Kerberos.
3. For using Kerberos, its libraries need to be used. The source should to be available to make such calls.
4. Kerberos never allow the unencrypted transfer of password but if required the Kerberos aware that it is just at own risk.

IV. PROBLEM STATEMENT

Cloud computing is one the most widely used of network. Some use its services, while other use it platform. The accessing should be such that the servers are available at some other location. Cloud providers initially taken into account also accessing but not the security. Thus some mechanism should be their which will provide security to cloud users and servers. This security should be in the form that it provides security features like authentication, non-integrity, availability. The security should provide features like encryption.

Authentication is mechanism of assuring that the request is from the intended sender only and no interference by any intruder is performed. If sender and receiver doesn't have any way of getting the assurance of trust between both then no third party will be capable of providing as well. Authentication is the method with dependency of asset value and risk. Just authentication is no much secure. Some Weak Authentication is the authentication between third parties. In security if not provided properly is always risk to the user. With increase in risk the security threat enhances. The factor should be kept in mind of researchers and certain protocol are designed. Hence authentication is very much required in safety of account.

There are many security mechanism applied in it. Integrity and several other security mechanisms. Certain techniques are used like password based, the password although can be tracked. Authentication mechanism involved variety of security like social security, third party security.

Our work observes that Kerberos is very good technique for enhancing the authentication. The demand is to have Kerberos in cloud computing.

V. SOLUTION DOMAIN

As the need is, find that there is strong need for security. The need is that strong cloud computing policy with best authentication scheme should be present. In our solution, the Kerberos is used as authentication scheme to have better authentication then user and password. In our approach the hybrid security is used. Here KDS have AS authentication server and TGS which is ticket granting server. Thus in our work the scheme is created which should have higher security to have authentication. In all the cloud based models the cloud server and client should have proper secure communication. The fine grain access control is the need of the architecture. Homomorphic encryption is designed along with the unique access structure. Access privilege and content which should be save form cloud servers.

Data isolation issues can be overcome in our work by avoiding the security breach of authentication.

The work analyzed the resources, which can be used by multiple providers. Our work enhance security by having TGS and AGS in it. It also provides features like accountability. The grant and revoking of request is given to user. Hence our solution is one step ahead of simple authentication.

A block diagram to represent the same is shown in Fig.4.

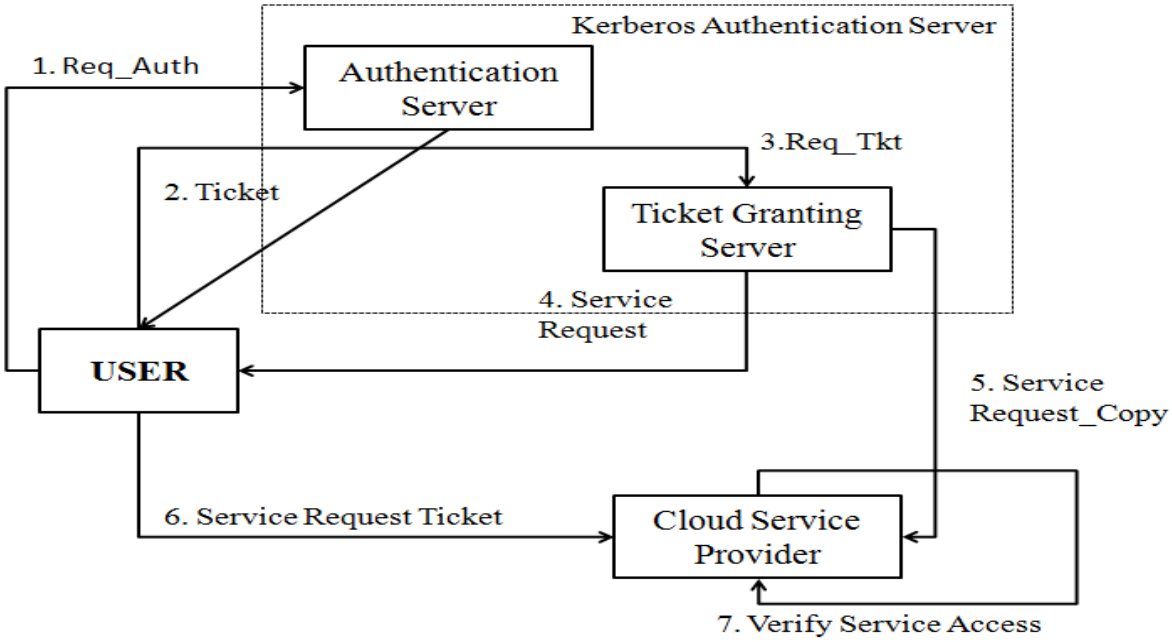

Fig.4. System Architecture.

VI. CONCLUSION

As we conclude that security is basic need of the cloud. The given work implements Kerberos to achieve authentication for having better security. Kerberos can be merging with ticket granting approach in order to achieve security. Here in our work we suggest security it in cloud-based architecture. Future work on this paper can be given as calculation of computation time and other factors as well as implementation of given solution.

REFERENCES

[1]. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", "*International Conference on Computer Science and Electronics Engineering*", 2012.

[2]. Tumpe Moyo, and Jagdev Bhogal, Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems, 2014.

[3]. Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", "System, Process and Control (ICSPC), 2014.

[4]. 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.

[5]. Cindhamani, NaguboyniaPunya, RashaEalaruvi, L.D. Dhineshbabu, "An enhanced data security and trust management enabled framework for cloud computing systems", *Computing, Communication and Networking Technologies* (ICCCNT), 2014.

[6]. Mrudula Sarvabhatla, Chandra Mouli Reddy M, Chandra Sekhar Vorugunti, "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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Anand Motwani, Rakhi Chaturvedi, and Anurag Shrivastava (2016). "Profit Based Data Centre Service Broker Policy for Cloud Resource Provisioning",*International Journal of Electrical, Electronics and Computer Engineering,* **5**(1): 54-60.

[12]. Javed Akhtar Khan and M.R. Alony, (2015). "A New Concept of Blood Bank Management System using Cloud Computing for Rural Area (INDIA), *International Journal of Electrical, Electronicsand Computer Engineering* **4**(1): 20-26.

[13]. Monika and Gurpreet Kaur (2016). "Enhancement in Sharing of Records on Secure Cloud using Advanced Encryption Standard and RSA", *International Journal of Electrical, Electronics and Computer Engineering*, **5**(1): 41-45.

[14]. Dr. Pawan Thakur and Sachin Awasthi (2017). "Infrastructure as a Service (IaaS) Security issues in cloud Computing", *International Journal on Emerging Technologies* **8**(2): 01-06.

[15]. Sachin Awasthi, Priyanka Thakur and Dr. Pawan Thakur (2016). *"Cloud Computing : A Comprehensive View*", *International Journal of Electrical, Electronics and Computer Engineering*, **5**(2): 11-15.