ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Enhanced Cloud Security through KFAC

Mahesh S Darak, Dr. N. K. Deshmukh

Assistant Professor, School of Computational Sciences, S. R. T. M. University, Nanded, Maharashtra, India

ABSTRACT: The current era is an era of high speed technology devices. To keep pace of devices the requirement for its processing & working is getting difficult with older and un-updated systems. For small and medium organization it is not possible to spend more & more revenue on the new & update infrastructure & services at regular intervals. To overcome all such problems there came a solution, known as cloud computing. The rapid growth in use of cloud computing has increased its security problems. To confront with such kind of security problem there is model proposed in this paper. Kerberos protocol is an authentication protocol in which client & server can authenticate each other across the insecure network connection Biometric is having its remarkable identity for identification & authentication of users. This paper proposes a new fusion model of Kerberos (K) and Fingerprint Authentication (FA), Cloud (C) which is known as Kerberos & Fingerprint Authenticated Cloud (KFAC) model.
.

KEYWORDS: Kerberos (K), Fingerprint Authentication (FA), Cloud (C), TGS (Ticket Granting Server).

I. INTRODUCTION

One of the hottest issue in the IT industry well known for its services is the cloud computing. Irrespective of location of the resources the different services can made available to the user through cloud computing.

The view towards cloud is always varying depending on the perspective of the individuals like on-demand model which make easy access to data when ever required. Cloud computing means a real time internet based information technology services that certify users' needs without the users having to pay maintenance and infrastructures cost. Cloud computing offers a wide range of services to organizations and businesses in a transparent manner over a large network like the internet [1].Internet and remote servers are used to maintain data and applications in cloud computing. Regardless of different benefits of cloud computing the major challenge is of security which consists of faith and access management. The cloud services are generally provided by the third party and the major issue of data security matter a lot in the process of data entry and retrieval by the authenticated and authorized users. To overcome all such security and privacy problems in usage of cloud computing the new model is been proposed named as KFAC (Kerberos and fingerprint Authenticated Cloud).

1.1 Cloud Computing:

Cloud computing is a new and emerging information technology that changes the way IT architectural solutions are put forward by means of moving towards the theme of virtualization: of data storage, of local networks (infrastructure) as well as software. The success of modern day technologies highly depends on its effectiveness of the world‘s norms, its ease of use by end users and most importantly its degree of information security and control. International Data Corporation (IDC) conducted a survey of IT executives and their line-business colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest challenge or issue of cloud computing [2].

Cloud has the option of pay per use annuity payments where in large upfront capital investment in IT infrastructure can be converted into smaller units based on requirement. The best starting point to think of the cloud is internet. User just logs in to his computing device. Cloud is a new computing paradigm that opens the door to bold new possibilities. Cloud will change the way the world works, plays, lives and learns. Enterprises have started moving their whole servers, applications on the cloud to ensure 24/7 access, improved customer experience, pay as peruse which helps in cost cutting, interoperability and scalability. Cloud computing has taken it to new heights with flexible scalable computing to match industry demand while reducing capital expenditure. Cloud computing provides different services rather than a unit of product.

DOI: 10.15680/IJIRCCE.2015. 0311137

1.2 Kerberos

Kerberos is an authentication protocol, and at the same time a (KDC), that has become very popular. Several systems including Windows 7 use Kerberos. Kerberos is named after the three headed dog in Greek mythology that guards the gates of l-Iades. Originally designed at Massachusetts Institute of Technology eM IT), it has gone through several versions. It was developed as a part of Project Athena at MIT to provide a solution to network security problems. Consider a distributed environment having many users on different workstations and services, available on servers distributed across the network. An unauthorized user may be able to gain access to services and data that he or she is not authorized to access. Instead of building elaborate authentication protocols at each server, Kerberos provides a centralized authentication server, whose function is to authenticate users to servers and servers to users.

Kerberos is an authentication protocol for trusted hosts on untrusted networks. The Kerberos protocol is designed to provide reliable authentication over open and insecure network where communicates between the hosts belonging to it may be intercepted. The following requirement for kerberos is: Secure-Reliable-Transparent-Scalable.

1.2.1. Authentication service AS: an authentication service that knows the password of all user and stores these in a centralized database in addition, the AS shares a unique secret key with each server.

1.2.2 Tickets granting service (TGS): TGS provide and issue tickets to user who have been authentication to AS.

1.2.3 Data Base: The kerberos server must have the user ID(UID) and hashed password of all participating user in the database .All user are register with the kerberos server. It makes more security in cloud server [3].

1.3 Biometrics

BIOMETRIC identification, or biometrics, refers to the process of identifying an individual based on his or her distinguishing characteristics. It comprises methods for uniquely recognizing humans based on one or more intrinsic physical or behavioral traits [5], [6].

There are three (3) traditional ways of authenticating the identity of an individual, these include

1) Possessions (such as keys, passports, and smartcards),

2) Knowledge (user ID, passwords and pass phrases), and

3) Biometrics.

These three modes of authentication can be combined, especially in automated authentication e.g. a password plus a user ID, an ATM card requiring a PIN, a passport with a face picture and signature biometrics, etc. [5].

In biometrics, there are two distinct authentication methods and they are:

1. Verification: It is based on a unique identifier which singles out a particular person (e.g. an ID number) and that individual's biometrics. It is based on a combination of authentication modes.

2. Identification: It is based only on biometric measurements. It compares these measurements to the entire database of enrolled individuals instead of just a single record selected by some identifier.

Biometric	**Identify versus Verify**	**Robust**	**Distinctive**
Fingerprint	Verify	**Moderate**	**High**
Hand/Finger Geometry	Verify	Moderate	Low
Facial Recognition	Either	Moderate	Moderate
Voice Recognition	Verify	Moderate	Low
Iris Scan	Either	High	High
Retinal Scan	Either	High	High
Dynamic Signature Verification	Verify	Low	Moderate
Keystroke Dynamics	Verify	Low	Low

Table: Comparison Table of Biometrics

1.3.1 Fingerprint Authentication:

Fingerprint recognition is also called as fingerprint authentication. It is a most popular biometric solution, refers to the automated method to confirmation the identity. Fingerprint authentication is popular among people because it inherent eases in acquisition. The fingerprint Authentication is well known and widely used at many places for authentication purposes. Fingerprint recognition verification or identification, are eventually based on a well-defined representation of a fingerprint

- One to One Matching: - It is applied where Input fingerprint is matched directly with only one fingerprint, which produces result either matched or not matched. Example: Secure Login using EmailID, Laptop & Desktop Device Protection, etc.
- One to Many Matching:- It is applied to specified areas where number of applicant store their fingerprint. The Input fingerprint is matched with number of fingerprint stored to uniquely find person identity. Example: Attendance Management, Secure Login without using EmailID, etc.
-

Nowadays, fingerprint recognition is one of the most important biometric technologies based on fingerprint distinctiveness, persistence and ease of acquisition.

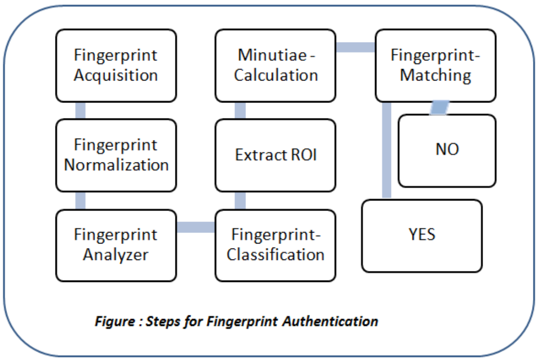

Figure : Steps for Fingerprint Authentication

II. RELATED WORK

2.1 Kerberos for cloud Computing: Kerberos is used for providing authentication for a client who want to access the applications stored at server side. Some another reasons for using Kerberos is, in Kerberos user password never travel over the network, never stored in any form on the client machine and it never be stored in unencrypted form and mutual authentication. Awareness of authenticity of user and server to each other is known as Mutual authentication.

Authentication Server: AS Issues a Ticket Granting Ticket to user. User sends their user name to server. Server responds with TGT encrypted with user's password. User enters password on client-if correct the TGT is successfully decrypted.

Ticket Granting Server: Logically different from the AS but may reside on the same server. User contacts when a network service is desired. Service ticket request is encrypted with session key provided by the in the TGT, not user's password.TGS authenticates tickets and issues a ticket for the resources as well as the encryption key to use with communication with the service.

Network Server: Client sends resource ticket and authenticator to the service encrypted with the client/server key. Server verifies both and issues a return message with a modified version of timestamp in the authenticator encrypted with client/service key. Client views message- if timestamp is modified correctly the service is genuine and ready to process request.

Since all authentication is controlled by a centralized Key Distribution Centre, compromise of this authentication infrastructure will allow an attacker to impersonate any user by getting the knowledge about the key. So we use Threshold Cryptography algorithm to divide Ticket Granting Server into multiple parts to allow multiparty authentication, it means one cannot decrypt the key until the predefined numbers of parts of TGS are not available. Second reason for using Threshold Cryptography algorithm is to provide more availability to the TGS. In a traditional Kerberos authentication system if TGS got deactivated due to any reason, then all the system get affected and the whole procedure of authentication get shut down. To avoid this type of system failure in this paper we are proposing a Threshold Cryptography algorithm which will divide our TGS into n parts and at least k parts are need to make an useful information. Here k is always smaller than n[7].

Advantages of Kerberos Authentication

1. **Mutual Authentication:** When two nodes -- such as a client and server or server and server -- begin communications, they pass encrypted tickets through a trusted third-party system called the Key Distribution Center. The KDC passes a secret ticket with a decryption key to both nodes. The nodes then pass encrypted time stamps to each other and use the key to decrypt them. If they do so successfully, they authenticate their counterparts and can trust each other for as long as the session remains open.
2. **Passwords:** When a server attempts to authenticate a client computer using the Kerberos protocol, the client does not have to send a password -- thanks to the mutual authentication, both the client and the server have the necessary information needed to decrypt the tickets. This means that any packet sniffers eavesdropping on the communication will not have access to client or server passwords, let alone any other information passed during the session.
3. **Integrated Sessions:** When a client node is authenticated on a Kerberos-supported network, it receives a client ticket with an expiration time stamp. As long as the ticket has not expired, the client can use it to access to any other network service that supports Kerberos authentication without having to re-authenticate itself. If the client's session on the network is still active but the ticket expires, the client may request a new ticket.
4. **Renewable Sessions:** Once a client and server have authenticated themselves to one another, they never have to do so again. As part of the mutual authentication, the client receives credentials from the server. When the client initiates a future session, it sends its credentials to the server, which recognizes them and immediately authenticates the client. This eliminates the need for a KDC, so the two nodes can establish a secure connection even faster than they did during their first session [9].

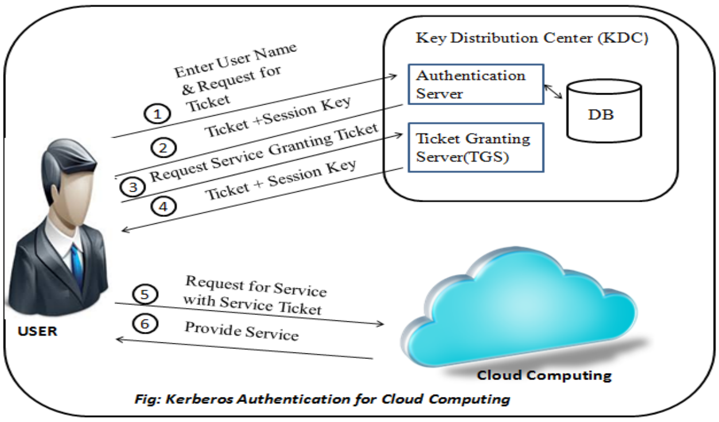
Key Distribution Center (KDC)
Authentication Server
DB
Ticket Granting Server(TGS)
1
Enter User Name & Request for Ticket
2
Ticket +Session Key
3
Request Service Granting Ticket
4
Ticket + Session Key
5
Request for Service with Service Ticket
6
Provide Service
USER
Cloud Computing

Fig: Kerberos Authentication for Cloud Computing

2.2 Fingerprint Authentication for Cloud Computing:

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the foot can also leave an impression of friction ridges. Finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier. Fingerprints of an individual have been used as one of the vital parts of identification in both civil and criminal cases because of their unique properties of absolute identity. Fingerprint-based personal identification has been used for a very long time [8]. Owning to their distinctiveness and stability, fingerprints are the most widely used biometric features. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Since fingerprint authentication is cheapest biometric authentication method and due to its robustness it more rapidly been used for cloud security.

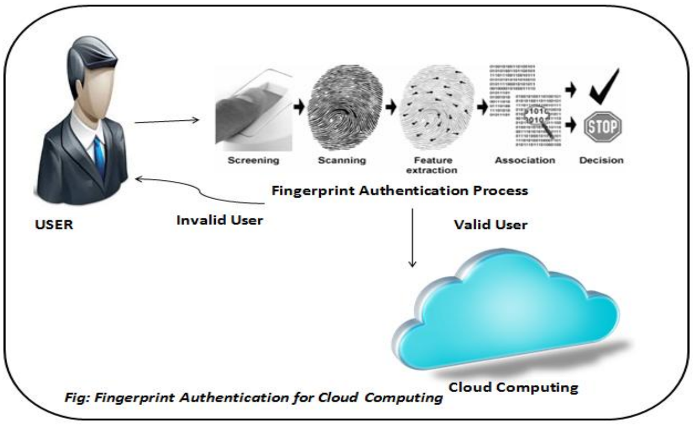

Fig: Fingerprint Authentication for Cloud Computing

Advantages of Fingerprint Authentication

1. Very high accuracy.
2. Is the most economical biometric PC user authentication technique.
3. Easy to use.
4. Small storage space required for the biometric template, reducing the size of the database memory required.
5. It is standardized.

III. PROPOSED MODEL KFAC

The proposed KFAC model is a hybridization of Kerberos model as well as fingerprint authentication for cloud computing. Proposed model KFAC is the hybridization of Kerberos and Fingerprint Authentication it is also known KFAC model (Kerberos with fingerprint Authentication Cloud). In kerberos authentication model the user first sends the username and demands the ticket for the accession of the services. Then the authentication server sends a ticket and session key to the user. Then using that ticket provided by authentication server the user request for the service granting ticket to the ticket granting server (TGS). Then the TGS grants the service ticket to the user with which user can avail the desired services. In fingerprint authentication model the user authentication is checked using their fingerprint there are several biometric methods for authentication checking but the well known and the cheapest one is the fingerprint authentication. In fingerprint authentication there are some steps like screening, scanning, feature extraction association and decision. There are various algorithms available for the fingerprint authentication. To overcome various problems in Kerberos authentication & fingerprint authentication individually the hybridization of both the authentication model together will jointly solve the problems which individual were not able to overcome. The proposed model KFAC will work as follows

1) The user will send username ,request for ticket & fingerprint to the Authentication server of KDC
2) The authentication server will check the user validity using fingerprint and the username
3) If the provided fingerprint is authentic then & then only user will get the ticket for demanding the service ticket to TGS (Ticket Granting System).
4) If user is valid then using the ticket granted by authentication server user will request for the service ticket to the TGS.
5) After getting the service ticket from the TGS the user can easily avail the cloud services.

In traditional Kerberos system any person who knows the user name could get the ticket from the authentication server & further from the TGS which could result in misuse of the services as well as security violation but due to proposed KFAC model only the registered users having username as well as their fingerprint registered to KFAC will be able to access the services for which authentication were required.

Advantages of KFAC

1. **Secured KFAC -** It provides secured access to cloud computing using Kerberos & fingerprint Authentication

2. **Ease of Use -** the user can have quick access to data based on the correct fingerprint & using tickets.
3. **Secure Authentication** -Fingerprint Authentication used with the Kerberos authentication helps to identify the correct user to use the services.
4. **Hybridization -**The hybridization will remove most the setbacks of an individual system**.**
5. **Robust System-** The Kerberos authentication has become robust due to only authenticated user are able to access the service tickets.
6. **Accountability** – The KFAC restricts access to clouds, protects data on cloud and provides audit trail minimizing misuse for the third party (i.e. Cloud Vendors).

IV. SIMULATIONS & RESULTS

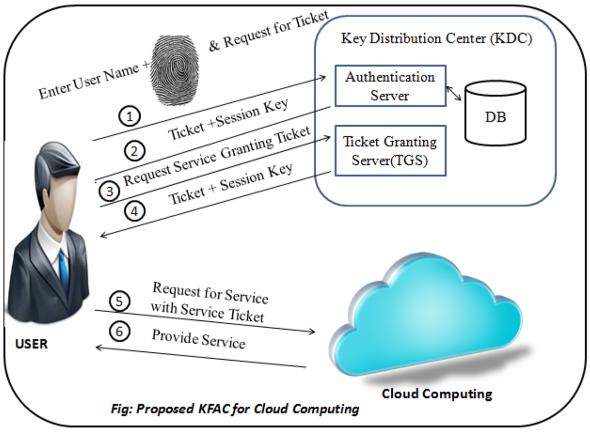
Enter User Name + & Request for Ticket
Key Distribution Center (KDC)
Authentication Server
DB
Ticket Granting Server(TGS)
1
Ticket +Session Key
2
Request Service Granting Ticket
3
Ticket + Session Key
4
USER
Request for Service with Service Ticket
5
Provide Service
6
Cloud Computing

Fig: Proposed KFAC for Cloud Computing

The result of implementing KFAC is an secured and authenticated use of cloud computing by giving access to authorised users only.

V. CONCLUSION

The acceptance of cloud Computing has been rapidly more in demand due to which the security issues of cloud has to be taken more in account. To keep the cloud computing secured and more authentic based the hybridization of Kerberos with Fingerprint authentication also known as KFAC will help to keep more of the accountability of access being provided only to the authenticated authentic users. In this paper we have seen different authentications models like Kerberos and Fingerprint authentication for security with their characteristics advantages & disadvantages. KFAC is proposed model for access control and security of cloud computing. KFAC model is extended model for both Kerberos & Fingerprint Authentication for cloud computing.

REFERENCES

1. Habib, S.M. Ries and S. Muhlhauser, “Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation” in Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), Oct. 2010, pp. 410-444.
2. Mahesh Darak,”Cloud Refuge through Iris Security (CRIS)”, IJAMTES, Vol. III, issue 4(II), January 2014, ISSN: 2249-7455.
3. Mehdi Hojabri,” Ensuring data storage security in cloud computing with effect of kerberos “, IJERT, ISSN: 22780181, Vol: Issue 5, July 2015.
4. Mahesh S .Darak, Dr. V. P. Pawar, Supriya Lohiya, Sapna Darak” Cloud Computing & its Applications in various sectors”, Asian Journal of Management Sciences 02 (03 (Special Issue)); 2014; 07-11.
5. Yuvraj Gupta “Enhancing Data Security in Cloud Computing” International Journal of Scientific & Engineering Research, Volume 3, Issue 12, December-2012, ISSN 2229-5518.
6. Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, and Andrew W. Senior, Guide to Biometrics. Springer Science + Business Media, Inc, NY 10013, USA, 2004, pp 3 – 6, 31 – 45, 146 – 148.
7. Shubha Bharill, Praveen Lalwani, T.Hamsapriya,” A Novel Approach for Enhancing the Authentication Process in Cloud Computing” ELSEVIER , Proc. of Int. Conf. on Advances in Computer Science, AETACS 2013.

8. Kalyani Mali , Samayita Bhattacharya,” Fingerprint Database Handling Using Cloud Computing With Added Data Mining and Soft Computing Features”, ijetae, ISSN 2250-2459, Volume 3, Issue 2, February 2013.

9. http://science.opposingviews.com/advantages-kerberos-authentication-4863.html as on date 27/11/2015.

10. Mr. Mahesh Darak , Dr. V. P. Pawar,” Cloud Computing Based e- -learning Model (CCBEM) for Distance Education through Open University’s, IJARCSSE, Volume 4, Issue 5, May 2014 ISSN: 2277 128X.