Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Data Privacy & Security Model for Cloud Computing

Mr. Mahesh Darak
Assistant Professor[1], School of Computational Sciences, S. R. T. M. University, Nanded, Maharashtra, India

Abstract: In the current era each and every size of business whether it is small, medium or big size of enterprise each and every one in preferring cloud computing for economical benefits. Cloud computing is having several advantages like on demand services, flexibility, Resource pooling, etc but due to its security and other challenges

are only problem or difficulty that must overcome in wide adoption of cloud computing. To overcome the security problem up to a certain extent the proposed model in the paper is a combination of Kerberos & more than one biometric for authentication.

Keywords: *Cloud Computing, Security, Biometrics, Iris, fingerprint.*

1. INTRODUCTION

One of the newest 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. To overcome all such security and privacy problems in usage of cloud computing the new model is been proposed combination of Kerberos Authentication and Biometrics (i.e. IRIS).

1.1 Cloud Computing:

"Clouds are a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized service-level Agreements"

Cloud computing is a kind of computing system in which various hardware, software and applications share their facilities over the internet. In general cloud computing is a technology based on virtual technology. It is a technology in which virtual techniques are used to perform many tasks through the use of Internet only. Cloud computing is the technology which can be used only through internet. It provides a strong mechanism for retrieving the information by the advance computing and the virtual technology with the use of information technology. Cloud computing acts as central remote server to update the information and maintain data records. It gives the rights for storage and process of centralized data. So far, for the effective use of cloud computing, we require internet connection by the cost effective service of computing [2].

1.2 Service Models: Cloud Services made available to users on demand via the Internet from a cloud computing provider's.

1. Software as a Service: SaaS is a complete operating environment with applications, management, and the user interface. In the SaaS model, the application is provided to the client through a thin client interface (a browser, usually), and the customer's responsibility begins and ends with entering and managing its data and user interaction. Everything from the application down to the infrastructure is the vendor's responsibility.

2. Platform as a Service: PaaS provides virtual machines, operating systems, applications, services, development frameworks, transactions, and control structures. The client can deploy its applications on the cloud infrastructure or use applications that were programmed using languages and tools that are supported by the PaaS service provider. The service provider manages the cloud infrastructure, the operating systems, and the enabling software. The client is responsible for installing and managing the application that it is deploying.

3. Infrastructure as a Service: IaaS provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets as resources that clients can provision. The IaaS service provider manages the entire infrastructure, while the client is responsible for all other aspects of the deployment. This can include the operating system, applications, and user interactions with the system.

4. Hardware as a Service (HaaS): In Hardware as a Service (HaaS) user of the service leases the hardware for his own purposes. This option allows you to save on maintenance of the equipment, but in essence little different from "Infrastructure as a Service" except that you have the bare hardware on which you can deploy your own infrastructure using the most appropriate software.

1.3 Types of clouds: There are different types of clouds that you can subscribe to depending on your needs. As a home user or small business owner, you will most likely use public cloud services.

1. Public Cloud –A Public cloud is open cloud which allows general public to easily access system and services, e.g., e-mail.

2. Private Cloud - A private cloud is a cloud in which an organization is allowed to avail systems and services. It offers more security since its private in nature.

3. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community. However its important activities are performed using private cloud and other activities using public cloud.

4. **Community Cloud** - A community cloud is shared among two or more organizations that have similar cloud requirements.

1.3 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.

1.3.1. 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.

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

1.3.3 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].

1.4 Biometric Fingerprint & Iris Authentication

Biometric Encryption The word biometric is originated from Greek language and which refers the identification of human by their unique measurable biological characteristics. The common physical characteristic used for security purpose are finger print, eye, voice, hand and face. Here we use physiological measurements. Since they are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. Biometric identification consists of two stages: enrollment and verification. During the enrollment stage, a sample of the designated biometric is acquired. Some unique characteristics or features of this sample are then extracted to form a biometric template for subsequent comparison purposes. During the verification stage, an updated biometric sample is acquired. As in enrollment, features of this biometric sample are extracted. These features are then compared with the previously generated biometric template [4].

The biometric systems based on behavioral characteristics fail in many cases as the characteristics can easily be learnt and changed by practice. Some of the techniques based on physiological characteristics such as Face Recognition, Finger Prints and Hand Geometry also fail when used over a long time as they may change due to ageing or cuts and burns.

Fingerprint-based identification is one of the oldest biometric techniques. A fingerprint consists of three-dimensional lines called ridges and the spaces between them are called valleys. Fingerprint identification is different from fingerprint verification. In identification, the question is to answer whose fingerprint is this. In verification, the question is, are you who you claim to be. In fingerprint identification, a large database has to be searched and match is of a form 1:N, whereas in verification the original image is to be matched with the live scan image and the match is of 1:1 form. Time required for identification is much larger than the time for verification.

Iris recognition system can be used to either prevent unauthorized access or identity individuals using a facility when installed, this requires users to register their irises with the system. A distinct iris code is generated for every iris image enrolled and is saved within the system. Once registered, a user can present his iris to the system and get identified. Iris recognition technology to provide accurate identity authentication without PIN numbers, passwords or cards. Enrollment takes less than 2 minutes. Authentication takes less than 2 seconds . Among all the biometric techniques Iris Recognition has drawn a lot of interest in Pattern Recognition and Machine Learning research area because of its several advantages.

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

2. 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.

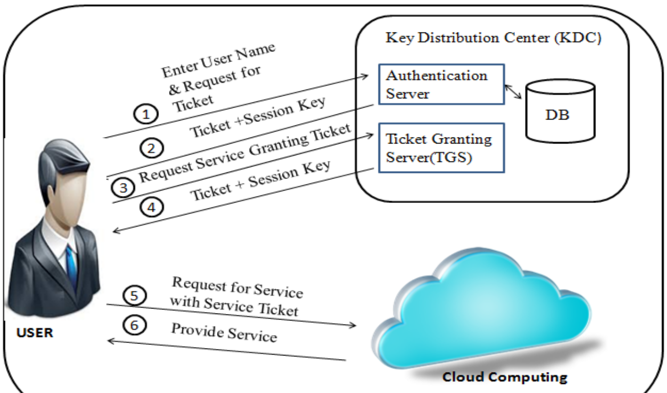
Key Distribution Center (KDC)
Enter User Name & Request for Ticket
1
Authentication Server
DB
Ticket +Session Key
2
Request Service Granting Ticket
3
Ticket Granting Server(TGS)
Ticket + Session Key
4
USER
Request for Service with Service Ticket
5
Provide Service
6
Cloud Computing

Fig: Kerberos Authentication for Cloud Computing

2.1.1 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.

2.1.2 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.

2.2.3 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[5].

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 [6].

2.2 Fingerprint Authentication

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 [11]. 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.

2.3 Iris Authentication: The Iris Verification system can be split into four stages: data acquisition, segmentation, encoding and matching. The data acquisition step captures the Iris images using Infra-Red (IR) illumination. The Iris Segmentation step localizes the Iris region in the image. For most algorithms and assuming near-frontal presentation of the Pupil, the Iris boundaries are modeled as two circles, which are not necessarily concentric. The inner circle is the pupillary boundary between the Pupil and the Iris whereas the outer circle is the limbic boundary between the Iris and the Sclera. The noise due to Eyelid occlusions, Eyelash occlusions, Specular highlights and Shadows are eliminated using segmentation. Most segmentation algorithms are gradient based that is segmentation is performed by finding the Pupil-Iris edge and the Iris-Sclera edge. The encoding stage encodes the Iris image texture into a bit vector code. The corresponding matching stage calculates the distance between Iris codes, and decides whether it is a match in the verification context or recognizes the submitted Iris from the subjects in the database. Biometrics is widely used in many applications such as access control to secure facilities, verification of financial transactions, welfare fraud protection, law enforcement, and immigration status checking when entering a country.

Advantages of Iris Authentication

1. The Iris formation starts in the third month of gestation period and is largely complete by the eight month and then it does not change after two or three years.
2. The human Iris might be as distinct as the iris for the different individuals.
3. The forming of Iris depends on the initial environment of the Embryo and hence the Iris Texture Pattern does not correlate with genetic determination.
4. Even the left and the right Irises of the same person are unique.
5. It is almost impossible to modify the Iris structure by surgery.
6. The Iris Recognition is noninvasive.

It has about 245 degrees of freedom [14].

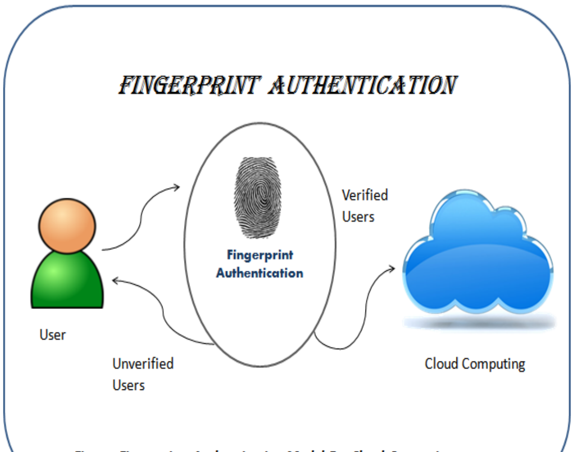

Figure: Fingerprint Authentication Model For Cloud Computing

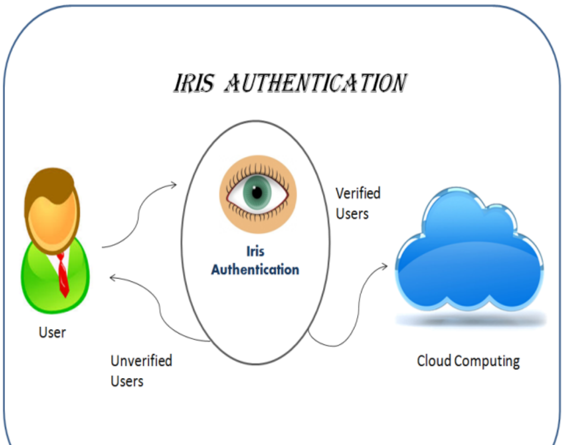

Figure: Iris Authentication Model For Cloud Computing

3. PROPOSED MODEL

Proposed model Kerberos Fingerprint & Iris authentication is the hybridization of Kerberos Fingerprint & Iris Authentication it is also known Kerberos Fingerprint & Iris authentication model (Kerberos with Fingerprint & Iris 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 & Iris authentication model the user authentication is checked using their Fingerprint & iris there are several biometric methods for authentication checking but the well known and the robust one is the Fingerprint & iris authentication. In iris authentication there are some steps like Image Capture, Eye localization, Iris Segmentation, Normalization process, feature extraction association and decision. There are various algorithms available for the iris authentication. To overcome various problems in Kerberos authentication & Iris 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 Kerberos Fingerprint & Iris authentication will work as follows

1) The user will send username ,request for ticket Fingerprint & Iris to the Authentication server of KDC
2) The authentication server will check the user validity using Fingerprint & Iris with the username
3) If the provided Iris 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 Kerberos and Iris authentication model only the registered users having username as well as their Iris registered to Kerberos and Iris authentication will be able to access the services for which authentication were required.

Advantages of Kerberos Fingerprint & Iris Authentication

1. **Secured KERBEROS AND IRIS AUTHENTICATION -** It provides secured access to cloud computing using Kerberos & Iris Authentication
2. **Ease of Use -** the user can have quick access to data based on the correct Iris & using tickets.
3. **Secure Authentication** -Iris 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 Kerberos and Iris Authentication restricts access to clouds, protects data on cloud and provides audit trail minimizing misuse for the third party (i.e. Cloud Vendors).

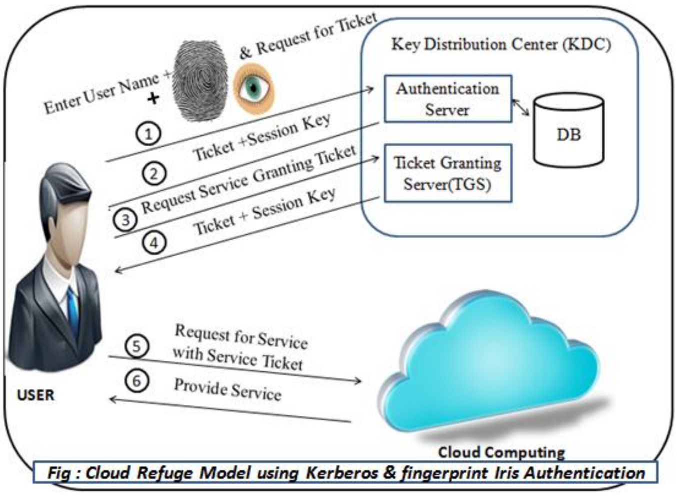
Enter User Name + + & Request for Ticket
Key Distribution Center (KDC)
Authentication Server
DB
Ticket Granting Server(TGS)
1
Ticket +Session Key
2
Request Service Granting Ticket
3
Ticket + Session Key
4
USER
5
Request for Service with Service Ticket
6
Provide Service
Cloud Computing

Fig : Cloud Refuge Model using Kerberos & fingerprint Iris Authentication

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 & Iris authentication also known as Kerberos Fingerprint & Iris Authentication 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 Fingerprint & Iris authentication for security with their characteristics advantages & disadvantages. Kerberos Fingerprint & Iris Authentication is proposed model for access control and security of cloud computing. Kerberos and Iris Authentication model is extended model for both Kerberos Fingerprint & Iris 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 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.

[3] Mehdi Hojabri," Ensuring data storage security in cloud computing with effect of kerberos ", IJERT, ISSN: 22780181, Vol: Issue 5, July 2015.

[4] Bhargava R, Pramoda R & Sudhakara Reddy M, " Dynamic RBAC Model for Cloud Computing", NCETCSE-2015, ISRASE explore Digital Library.

[5] 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.

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

[7] Mahesh Darak,"Cloud Refuge through Iris Security (CRIS)", IJAMTES, Vol. III, issue 4(II), January 2014, ISSN: 2249-7455.

[8] 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.

[9] http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20 technologies as on date 20/09/2015

[10] Himabindu Vallabhu, R V Satyanarayana "Biometric Authentication as a Service on Cloud: Novel solution" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012

[11] H. C. Lee and R. E. Gaensslen, Eds., Advances in Fingerprint Technology. New York: Elsevier, 1991.