ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Authorization Protocol and Pervasive Computing Environments Authentication in Cloud Computing

Pavan Nadagundla
Assistant Professor,
Department of CSE,
Malla Reddy Institute of Technology,
Maisammaguda, Hyderabad.

M.Naresh
Assistant Professor,
Department of CSE,
Malla Reddy Institute of Technology,
Maisammaguda, Hyderabad.

Abstract:
Cloud computing is a revolution in information technology. The cloud client outsources their sensitive data and personal information to cloud provider's servers which is not within the same trustworthy domain of data-owner therefore most difficult problems arises in cloud are data security users privacy and access control. In this paper we also have proposed a method to achieve fine grained security with combined approach of PGP and Kerberos in cloud computing. The projected method provides authentication, confidentiality, integrity, and privacy features to Cloud Service Providers and Cloud Users.

Keywords:
Cloud computing, security, access control, privacy, authentication, Pretty Good Privacy, Kerberos.

I.INTRODUCTION:
Cloud computing is a large-scale distributed computing paradigm that's driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services square measure delivered on demand to external customers over the Internet [1]. It is an Internet-based computing solution where shared resources/services are provided like electricity distributed on the electrical grid. The cloud computing offer basically three type of services. Software as a Service (SaaS) in which the cloud service provider provides applications and software over a network. Google Docs, Facebook, Gmail, Yahoo are the example of SaaS [2]. Platform as a Service (PaaS) provides application or development platform in which user will produce their own application that will run on the cloud, example of PaaS are Microsoft's Azure, Google's Application Engine (app engine), Yahoo Pig [3].

Third type available and might serve multiple tenants. samples of public cloud are: Google App Engine, servers, routers, hardware based load balancing, firewalls, storage and other network equipment is provided by the IaaS provider i.e. Amazon S3, Amazon EC2 [4]. Cloud computing can be deployed as public cloud, private cloud, hybrid cloud and community cloud. Public clouds are publicly available and can serve multiple tenants. Examples of public cloud are: Google App Engine, Microsoft Windows Azure, IBM Smart Cloud and Amazon [3] while private cloud is typically a tailored environment with dedicated virtualized resources for particular organization. Examples of private clouds are Eucalyptus, Ubuntu Enterprise Cloud–UEC, Amazon VPC (Virtual Private Cloud), vmware Cloud. Infrastructure Suite, and Microsoft ECI data-centre. Similarly, community cloud is tailored for a particular group of customers Google Apps for Government, Microsoft Government Community Cloud are the example of community cloud [3]. Hybrid cloud is composed of multiple clouds including public and private cloud like Windows Azure (capable of Hybrid Cloud), vmware v Cloud (Hybrid c loud Services)

II. LITERATURE REVIEW:
A novel privacy increased anonymous authentication and access management theme are projected to secure the interactions between mobile users and services in Pervasive Computing Environments (PCEs) with nonobligatory context authentication capability by integration of two underlying crypto graphical primitive's i.e. blind signature and hash chain, into a highly flexible and lightweight authentication and key establishment protocol [5]. It provides explicit mutual authentication and allows multiple current sessions between a user and a service,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

while allowing the user to anonymously interact with the service. The requirements of privacy and security for Pervasive Computing Environments (PCEs) are realized and analyzed that existing privacy-preserving access control schemes do not absolutely satisfy these necessities therefore planned two approaches towards privacy-preserving access control in PCEs to enhance privacy by achieving untraceability and unlinkability even against malicious insiders and additionally to reinforce security by achieving conditional traceability of user credentials [6]. An authentication and authorization protocol for anonymous communication in the cloud is proposed [7]. The protocol is an extension of existing standards making it easy to integrate and compatible with existing standards. The trust model of PKI along with others to highlight the different shortcomings of these models and proposed a number of features that should be present in an open network [8]. New password authentication schemes that support the Diffie–Hellman key agreement protocol over insecure networks are proposed [9]. A method of implementing two factor authentication using mobile phones is also proposed [10].The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner. An authentication based on sending one time password to registered mobile number is proposed [11]. The SMS system doesn't guarantee to deliver the token at real time. The data can still be intercepted by the malicious persons.

III.METHODS:

3.1 kerberos:

Kerberos is an authentication protocol for network security based on cryptography. It provides mutual authentication and message integrity as well as data confidentiality. It uses secret key cryptography, which proves identity of communicating parties over network, and also prevents eavesdropping or replay attacks [12]. Kerberos performs secure verification of users and services based on the concept of a trusted third party (KDC) [13].

Components of the Kerberos (Servers)

The Kerberos authentication system consists three servers i.e. Authentication Server (AS), Ticket Granting Servers (TGS) and real server (CSP) that provides services to others.

Authentication Server (AS)

It is the KDC in the Kerberos. Each user registered with AS and is granted a user identity and password and keep these credentials in its database of every individuals. AS verifies the user, issues a session key to be used between user and TGS.

Ticket Granting Servers (TGS)

It issues a ticket for the real server (B). It also provides the session key KAB between user (A) and real server (B). Real Server It provides services to the users. Units

3.2 Pretty Good Privacy (PGP):

PGP developed by Philip R. Zimmermann in 1991 [14]. PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. It is used in several security constraints such as confidentiality, integrity and authentication for electronic mail and file storage applications etc [15]. PGP exists in two public key versions- (RSA) and Diffie-Hellman [16]. In RSA version, PGP uses the IDEA algorithm to generate a short key for the entire message and RSA to encrypt the short key. The Diffie-Hellman (DH) version uses the CAST algorithm for the short key to encrypt the message and the DH algorithm to encrypt the short key. PGP uses a hash algorithm to send digital signature of sender to receiver. This digest is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the digest. If it matches the hash code sent as the digital signature for the message, then the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version uses the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version uses the SHA-1 algorithm to generate the hash code [16].

Working of PGP Message Encryption and Decryption PGP is a hybrid cryptosystem; it uses the best features of conventional and public key cryptography. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and public key cryptography; each step uses one of several supported algorithms [15]. Data Encryption: One-time-only secret key generation PGP first creates a one-time-only secret key that is called session key which is a random phrase. This session key works with IDEA to encrypt the plaintext which is a very fast and secure conventional encryption algorithm [17]. The session key is encrypted with the receiver's public key after the data is encrypted by session key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient[18].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Decryption:

This is the just reverse process of the encryption. The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted cipher-text.

IV THE HYBRID APPROACH TO AUTHENTICATION USING PGP AND KERBEROS:

Since Kerberos does not support non repudiation, this weakness of Kerberos can be reduce by applying public key cryptography and Digital Signatures, so PGP can deploy successfully with Kerberos because PGP supports public key cryptography Digital Signatures.

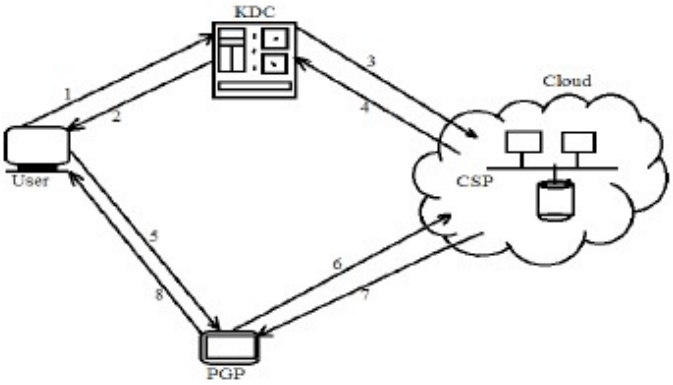

Figure 1. Proposed Method for Authentication for cloud

Step-1. User register his identity to Kerberos (KDC).
Step-2. KDC provides ticket to user to communicate withCSP.
Step-3. KDC also send a ticket and user identity to CSP, nowCSP stores these credentials for future use.
Step-4. CSP acknowledge to KDC about user's credentialsstorage.
Step-5. User encrypts his data before sending to cloud.
Step-6. PGP authenticate user and send information to CSP.also PGP send user's encrypted data to cloud.
Step-7. The CSP send the desired data to PGP requested byuser.
Step-8. The PGP decrypts the data and user authenticationinformation. if user is authorised to access that data the PGP send the decrypted data to user. Working of Kerberos in hybrid approach

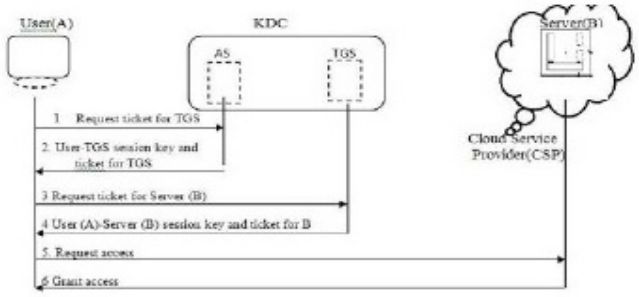

Figure 2. Kerberos Authentication of Cloud Service Provider.

Step-1: The user sends his request for service to AS.
Step-2: The AS sends a message encrypted with User's (A) permanent symmetric key, KA-AS. The message consists two items: a session key KA-TGS that is used by user A to contact the TGS and a ticket for the TGS that is encrypted with the TGS symmetric key KASTGS. User does not know the KA-AS, but when the message received, he types his symmetric password correctly then the appropriate algorithm together creates KA-AS. The password is destroyed immediately, it is not send to the network and it does not stay in the terminal. It is used for a moment to create KA-AS. Process now uses KA-AS to decrypt the message sent. KA-TGS and the ticket are extracted.
Step-3: User (A) now sends three items to the TGS. The first is the ticket received from AS and the second is the name of the real server (B) (i.e. Cloud Service Provider), and the third is a timestamp that is encrypted by KA-TGS. The timestamp prevents a replay by Eve.
Step-4: Now, the TGS sends two tickets, each containing the session key between user(A) and real server(B). KA-B, the ticket for user (A) is encrypted with KA-TGS; the ticket for server (B) is encrypted with B's public key KTGS-B. Note: Eve cannot extract KA-B, because Eve does not know KA- TGS and KTGS-B, even she cannot replay step-3 because Eve does not replace the timestamp with new one (she does not know KA-TGS).
Step-5: User (A) sends Server (B) ticket with the timestamp encrypted by KA-B.
Step-6: Real server B confirms the receipt by adding 1 to the timestamp. The message is encrypted with KA-B and send to user (A). Since PGP support digital signature and public key cryptography. After successful authentication by Kerberos the user (A) initiate the PGP for next authentication and data encryption process for confidentiality and data integrity.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Working of PGP in hybrid approach:

We know that the digital signature provides message authentication and integrity. So the sender (User) and the receiver (CSP) agree on the PGP.

Authentication and Integrity:

In authentication process, the sender first calculates the message digest of the data which figure illustrates the process of digital signature service provided by PGP.

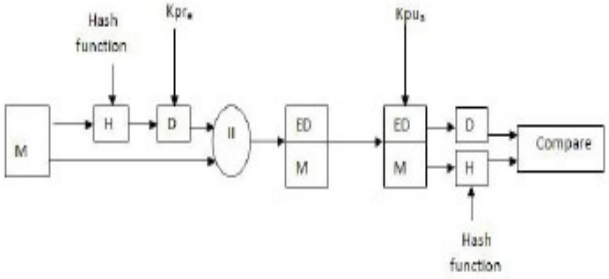

Figure 3. Authentication

Step-1. User calculates the message digest of the message.
Step-2. After calculating digest he encrypts this digest with his private key (put his digital signature).
Step-3: He concatenates the original message with encrypted message digest and sends to Cloud service provider. All these three steps are perform by user and next following steps are perform by Cloud Service Provider as
Step-4: After receiving the message from user in step-3 the CSP decrypts the digest with user public key and get the message digest.
Step-5: In step 5 the CSP calculate the message digest of the message received using same hash function.
Step-6 if both digest comparison calculated same; it shows that the sender is authentic user, whose public key is available to CSP repository. Also calculated digest show that the integrity of the message is uniform. Confidentiality.

The PGP provides confidentiality using several steps as follows
Step-1: User first compresses his message using appropriate compression algorithm and then encrypts the compressed message with a session key.
Step-2: After encrypting the compressed data the session key is also encrypt with public key of CSP.
Step-3: In step-3 the encrypted data and session key are concatenated and send it to the CSP.
Step-4: At CSP end after receiving data from user the CSP decrypt the session key using his private key and find session key.
Step-5: After getting session key, user decrypt the message using that session key and find the compressed message.
Step-6: After getting compressed data in step-5, the CSP uses appropriate decompression algorithm and find the original message. Figure shows the overall processes of confidentiality as

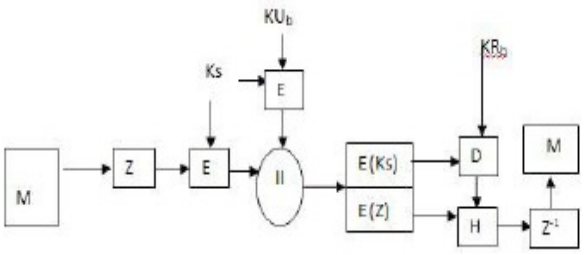

Figure 4. Confidentiality

V.SECURITY ANALYSIS OF PROPOSED FRAMEWORK:

1. Mathematical Attack: This attack will occur by determining p, q ornumbers-1)(q-1). It could be prevented by using 2048 bits exponents in RSA. Also it could be prevented by increasing the value of digest, the chance of successful mathematical attack would be decreased considerably.
2. User Privacy: The proposed scheme never transmits user private data in plaintext format. The messages are Transmitted over a public channel. Clearly, these messages cannot be decoded easily to get ID, PW etc. Hence, the Scheme provides user privacy.
3. Identity Management: In proposed method the KDC and CSP store all the registered IDs in the database and checks availability of a unique ID in each new registration and provide certificate to manage the identity of user.
4. Session Key Agreement: In proposed method, the secret key (K) is shared by the AS user and CSP. Using this Key they can communicate with each other for a particular session. Since this key is generated randomly it cannot be breach easily.
5. Security against Brute Force Attack: All possible combinations to guess the private key have been tried by the attacker during the brute force attack. In the original RSA, the probability of failure against this attack will be decreased Considerably by choosing exponents larger than 2048 bits.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

VI. CONCLUSIONS:

To achieve fine grained security in cloud, there are many ways and mechanisms similarly as ideas are proposed and Presented. In this concern here we propose a framework which uses Pretty Good Privacy (PGP) and Kerberos based security in cloud computing. Kerberos proves identity of users over networks and provides data integrity and secrecy. Kerberos performs secure verification of users and services based on the concept of a trusted third party (KDC).

VII.FUTURE WORK:

One of the weakness of Kerberos is that it cannot provides the non repudiation features in communication [19], so in future we will enhance this feature of non repudiation in our proposed work by using the Pretty Good Privacy program. We know that PGP uses the digital signature features in communication. PGP provides abilities to people to take their privacy into their own hands.

REFERENCES:

1] Foster, I., Zhao, Y., (2008). Cloud Computing and Grid Computing 360-Degree Compared. In: Grid Computing Environments Workshop (2008).

[2] Patel, S. C., Umrao, L. S. , Singh, R. S., Gupta, M. & Trived, N. (2013).Access Control Using Mobile Verification System For Cloud., International Journal of Information and Computation Technology(IJICT)ISSN 0974-2239 Volume 3, Number 1(2013)

[3] Patel, S.C., Umrao, L. S. & Singh, R. S. (2012). Policy-Based Framework for Access Control in Cloud Computing, International Conference on Recent Trends in Engineering & Technology (ICRTET2012) ISBN: 978-81-925922-0-6

[4] Mantri, A., Nandi, S., & Kumar, G. (2011). High Performance Architecture and Grid Computing, International Conference, HPAGC 2011,Springer.

[5] Kui Ren • Wenjing Lou "Privacy-enhanced, Attack-resilient Access Control in Pervasive Computing Environments with Optional Context Authentication Capability"

[6] Emmanouil Magkos, Panayiotis Kotzanikolaou, "Achieving Privacy and Access Control in Pervasive Computing Environments" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 00: 1–12 (2010)

[7] Umer Khalida, Abdul Ghafoor, Misbah Irum, Muhammad Awais Shibli,"Cloud based Secure and Privacy Enhanced Authentication & Authorization Protocol" International Conference in Knowledge Based and Intelligent Information and Engineering Systems - KES2013. Procedia Computer Science 22 (2013) 680 – 688.

[8] H. Liping, S. Lei, Research on trust model of pki, in: Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, Vol. 1, IEEE, 2011, pp. 232–235.

[9] Liao, I-E., Lee, C.-C. & Hwang, M.S. (2006). A password authentication scheme over insecure networks" Journal of Computer and System Sciences 72 (2006) 727–740,Elsevier.

[10] Aloul, F., Zahidi, S. & El-Hajj, W. (2009). Multi Factor Authentication Using Mobile Phones, International Journal of Mathematics and Computer Science, 4(2009), no. 2, 65–80.

[11] Choudhury A. J., Kumar P., Sain M.,Hyotaek L. andHoon J., "A Strong User Authentication Framework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific,2011.

[12] Srinivasa Rao Yarlagadda, Rupesh Shantamurty "Kerberos authentication made easy on OpenVMS", OpenVMS Technical Journal V18, http://h71000.www7.hp.com/openvms/products/kerberos/

[13] Gary C. Kessler, An Overview of Cryptography , Handbook on Local Area Networks1999 edition ,short edition, May2 .2014].

[14] Kamarudin Shafinah, Mohammad Mohd Ikram "File Security based on Pretty Good Privacy (PGP) Concept", Computer and Information Science, ISSN 1913-8989 E-ISSN 1913-8997, Vol. 4, No. 4; July 2011

[15] Michael Louie Loria "Pretty Good Privacy" http://slidedeck.io/michaellouieloria/pgp

[16] Margaret Rouse, "Pretty Good Privacy (PGP)" http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

[17] TIM CROOK "PGP AND ENCRYPTION",http://shrike.depaul.edu/~tcrook/DS420/pgp.html.