INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

RESULT PAPER ON A LIGHT AND RELIABLE AUTHENTICATION SCHEME ON CLOUD COMPUTING ENVIORNMENT

MS. NILAJA A. DESHMUKH[1], DR. H. R. DESHMUKH[2]

1. M.E (Scholar) Computer Science and Engg, I. B. S. S. C. O. E, Amravati.
2. Head Of Department, Computer Science and Engg, I. B. S. S. C. O. E, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Cloud computing is an emerging technology that is still unclear to many security problems. Ensuring the security of stored data in cloud servers is one of the most challenging issues in such environments. Cloud computing is a service oriented technology which provides various services to users which vary from software to hardware. However, ensuring the security in cloud computing environments is one of the most challenging issues. In cloud, when two parties communicate with each other, mutual authentication is needed for secure communication. This paper proposes a secure mutual authentication model for cloud environment. The authentication is handled by software-as-a-service application (ASaaS). Modified Diffie Hellman agent (MDHA) is used to provide mutual authentication which interacts with A SaaS instead of cloud server. The scheme provides authentication by using a four step process. Another agent named cryptography agent is used to provide encryption of data before uploading on the cloud**.** Authenticating users and establishing their identity is the first most part of any computer based application or website.

Keywords: Cloud computing, User Authentication agent, SaaS, Cryptography.

Corresponding Author: MS. NILAJA A. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Nilaja A. Deshmukh, IJPRET, 2016; Volume 4 (9): 982-988

PAPER-QR CODE

INTRODUCTION

Cloud computing is an emerging technology that is still unclear to many security problems and user authentication, access control, and ensuring the security of stored data in cloud servers are the most challenging issues in cloud-based environment. Accordingly, this paper offers an efficient and scalable user authentication scheme for cloud computing environment. It the suggested model, various tools and techniques have been introduced and used by using the concept of agent. Therefore, a client-based user authentication agent has been introduced to confirm identity of the user in client-side. [1][2]Cryptography agent was also introduced to encrypt resources before Diffie-Hellman is public key based symmetric key algorithm used for secret key sharing between two parties over public communication channel. Diffie-Hellman is weak when there is man in middle attack done by eavesdropper. Diffie-Hellman is modified to provide authentication and avoid primitive root generation step to achieve speed and authentication to avoid key exchange with unauthenticated user. Cloud is a third party service and so, a client cannot trust the cloud service provider to store its data securely within the cloud. So to avoid this insecurity of user's data there is a need to authenticate a client before using the services**.** Because of its high scalability, cloud computing offers unlimited computing resources on demand. This advance eliminates the need for the cloud service providers to plan far ahead on hardware provisioning [1]. Cloud computing has generated significant interest in industry, but it's still an evolving paradigm. Cloud computing attempts to combine computing technologies and the economic service model with the evolutionary development of several existing Users and the system can use the agreed session key to encrypt/decrypt their communicated messages using the symmetric cryptosystem.

1. LITERATURE SURVEY

The rapid growth in field of cloud computing communications in recent years also raises many researches in user authentication and access control models according to security issues in this unprecedented technology. In 2011, a strong user authentication framework for cloud computing was proposed by Choudhury *et al.* where user legitimacy is strongly verified before enter into the cloud by providing identity management, mutual authentication, session key establishment between the users and the cloud server [7]. In this model, two factors were chosen: one factor in "something you know" (*i.e.* password) and two factors in "something you have" (*i.e.* smartcard and OOB). According to evaluation the suggested framework can resist considerable attacks such as man-in-the-middle attack, replay attack, and denial of service attack [10][12]. In 2014, a scalable and efficient user authentication scheme was proposed by

Faraz Fatemi Moghaddam et al. in which two agents namely Client User Authentication (CUA) and Modified Diffie Hellmann (MDHA) are used for providing authentication to user while accessing data in cloud [5]. In 2014, a mutual authentication protocol was proposed by Sandeep Saxena et al. in which a shared key or group key is generated for mutual authentication and secure communication [1]. The proposed model uses the concept of identity based public key cryptography. The client registers his identity to central authority before starting communication. to implement user authentication down to the lowest (database) level. The complete security concept is domain independent and thus can be used for other cloud-based infrastructures. 2012 Seventh International Conference on Availability, service attack, man-in-the-middle attack [8]. Jaidhar C. D proposed an enhanced mutual authentication scheme for cloud computing environments in 2012 [4] which is resistant from insider attack, masquerade attack and password guessing attacks. This scheme provides mutual authentication between user and cloud server by agreeing upon a secret key and also the user can change password at smart card side without taking any permission from cloud authentication server.

3. PROPOSED MODEL

This section presents a proposed mutual authentication scheme for cloud environments. It is also known as two way authentication [9].The authentication process in the proposed model is separated from cloud servers and is (ASaaS) application. This reduces the load on cloud servers [5].

3.1 A. Client-Based User Authentication Agent (CUA*)* Client-based user authentication agent is an extension that has been installed in end-user's web browser to confirm the identity of user before accessing to cloud servers. Accordingly, user needs to register his devices on service provider website and download an extension with unique access code for installing on web browser. The unique code

will be encrypted by an optional password that has been chosen by user with AES-192 or AES-256 [9]

3.2. Modified Diffie-Hellman Agent (MDHA*)*

CUA provides a secure user authentication for personal and registered devices. However, for accessing to cloud servers with un-registered devices another process of authentication seems to be necessary. Accordingly, MDHA is introduced

based on ZKP Diffie-Hellman [20] to increase the rate of reliability in process of user authentication by un-registered devices. By using MDHA, temporary access permission has been provided for users for accessing from un-registered device. Table II shows this authentication in details.[9]

Table 1.Algorithm of Client-based user authentication

Client	Server
1 Registration Request(Com ID, Mac ID, User ID, access type*)	2. R=Check–the-Request (Com ID, Mca ID, access type*)If (R=yes)then Confirm-request.
3. Send optional password(PW)	4. ACG=Access Code Generation(), DL=Download Link Generation(), EAGG=Encryption(ACG,PW)end(DL.EACG)
5. Download extention(DL) **ACG=Decrypting(EACG,PW)**	

Table 2. Algorithm of Modified Diffie hellman Agent user authentication

Client	MDHa
1.Login(username, password)	2.L=check the login request(username, password) if (L=yes)then login status =approved define(large randam prime, P)define(large randam prime, G)define(integer x)R1*G mod P
3.Defibne(integer,Y) **R2=G^Y mod P** **K=R1^Y mod P** **E=encrypt(R2,K)** **Send(E,R2)**	
	4.K=R2^x mod P R2=decrypt(E,K) If(R2=R3)then login=status=confirmed Else login=status=rejected

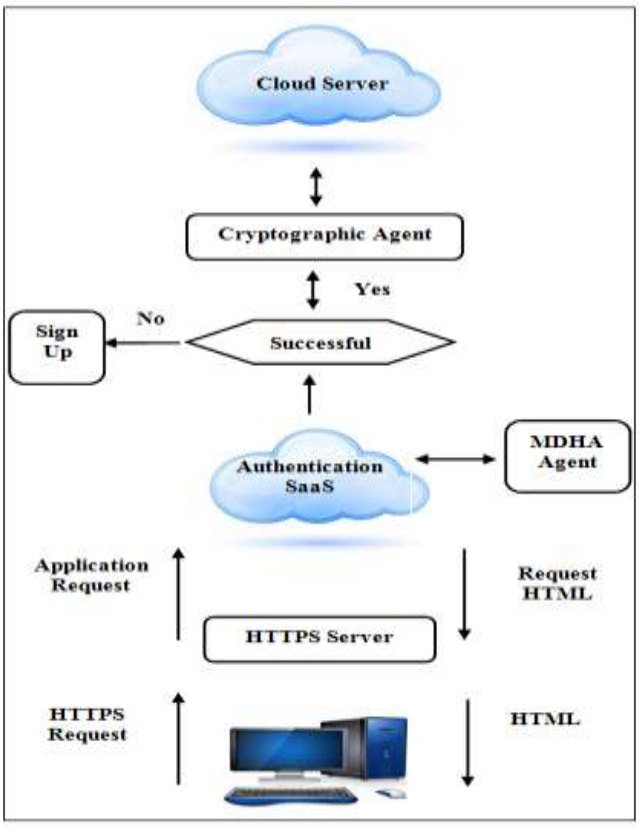

Figure no.1.

4. ADVANTAGES

4.1. Scalability: The suggested model uses various tools and techniques that make the cloud-based framework more scalable in comparison with related works. Using a client-based user authentication has decreased the dependency of this process to cloud-based operations considerably and by this decrease, the process of authentication will be more scalable

4.2. Security: By using various tools and techniques during authentication and also data protection processes, security of the suggested model has been improved.

4.3. Efficiency: The process of authentication in the suggested model has been more efficient by establishing logical and reasonable communications between various agents during the process of authentication.

5. CONCLUSION

It the suggested model, various tools and techniques were introduced and used by using the concept of agent. Therefore, a client-based user authentication agent was introduced to confirm identity of the user in client-side. In addition, cloud computing being a combination of computing resources; resource constrains are given less priority to provide high security to the cloud. Diffie Hellmann algorithm provides mutual authentication between server and user and interacts with A SaaS instead of mail cloud servers to decrease the load on cloud servers. The scheme prevents from many attacks like Man in the Middle attack, phishing attack. It also reduces complexity by using elliptic curve cryptography algorithm during both authentication and encryption process.

6. REFERENCES

1. B Wang et al, “Storing Shared Data on the Cloud via Security-Mediator”, IEEE 33rd International Conference on Distributed Computing Systems ISSN 1063-6927, 8-11 July, 2013, Page(s) 124-133,
2. L. B. Jivanadham et al, “Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism”, International Conference on Informatics, Electronics & Vision (ICIEV), Print ISBN: 978-1-4799-0397-9 17-15 May 2013, Page(s): 1 – 6.
3. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Communications of the ACM Magazine, vol. 53, no. 4, pp. 50–58, April 2010.
4. J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L.Montgomery, “On the security of 1024-bit rsa and 160-bit elliptic curve cryptography.,” IACR Cryptology ePrint Archive, p. 389, 2009.
5. J.-J. Shen, C.-W. Lin, M.-S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consumer Electron. 49 (2) (2003) 414–416.
6. J.-J. Shen, C.-W. Lin,M.-S. Hwang, Security enhancement for the timestamp-based password authentication scheme using smart cards, Comput. Secur. 22 (7) (2003) 591–595.
7. IEEE, P1363.2/ D23: Standard specifications for password-based public key cryptographic techniques, March 2006.
8. U. Somani, K. Lakhani, and M. Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,” in Proc. 1st International Conf. on Parallel Distributed and Grid Computing (PDGC), Solan, 2010, pp. 211-216.

9. Bo Zhao, Benjamin I. P. Rubinstein, Jim gemmell, and Jiaw Han, "A Bayesian approach to discovering truth from conflicting sources for data integration," pp. 550-561, August 2012.
10. Hellman, Martin E., (2002), "An Overview of Public Key Cryptography", IEEE Communications Magazine, May 2002, pp: 42-49.
11. S. J. Aboud, M. A. Alfayoumi, M. Alfayoumi, and H. Jabbar, —An Efficient RSA Public Key Encryption Scheme, ‖ in Proc. 5th International Conf. Information Technology: New Generations (ITNG),Las Vegas, 2008, pp. 127-130.
12. Curtmola, R., Garay, 1, Kamara, S., Ostrovsky, R. : Enhancing Detinition and Efficient Constructions using Searchable Symmetric Encryption In: 13th ACM Conference on Computer and Communications Security, pp. 79-88 (2006).
13. F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi, “A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments,” in Proc. IEEE 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, November 2013.