INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW PAPER ON USER AUTHENTICATION SCHEME ON CLOUD COMPUTING

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 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. In 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. Furthermore, a cloud-based software-as-a-service application has been used to confirm the process of authentication for registered & unregistered devices. In overall, the theoretical analysis of the suggested scheme shows that, designing of this model will enhance the reliability and rate of trust in cloud computing environment as an emerging and powerful technology in various industries.

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): 975-981

PAPER-QR CODE

INTRODUCTION

Cloud storage is an important service of cloud computing. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access[1] Authentication is any process by which a system verifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource so authentication is essential to effective Security. In other words, authentication often involves verifying the validity of at least one form of identification. Cloud computing as an emerging technology contains both the applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services [2].There are many concepts that have been used in cloud-based services that provide considerable benefits to end-users and also service providers. Unlimited storage for customers is one of the major benefits of cloud computing that reduce the concerns about the amount of remaining memory significantly.

A simple example of cloud computing is Yahoo email or Gmail, facebook, etc. Cloud computing comprises of three services: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS) Depending on the requirements, the customers can choose one or more services provided. This security has been divided to several parts and one of the most important parts is ensuring about the user authentication processes and managing accesses when users outsource sensitive data share on public or private cloud servers [4][5]. User authentication in cloud computing environments has been divided to two main processes: investigating unique identifiers of users during the initial registration phase, and user authentication and validating user legal identities and acquiring their access control privileges for the cloud-based resources and services during the service operation phase.Moreover, universal connectivity, open access, sustainability and interoperability are the other advantages of this newfound service [3]. However, Ensuring the security and privacy in cloud computing environments is one of the most challenging issues that decrease the rate of reliability in cloud-based products.

2. 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. 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] [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. MATERIALS AND METHODOLOGY

The algorithm is used to provide security in this sharing of personal record will be advanced encryption standard algorithm or RAS algorithm.

3.1 The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. Advanced Encryption Standard combination of both substitution and permutation, and is fast in both software and hardware.Unlike its predecessor DES, AES does not use a specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

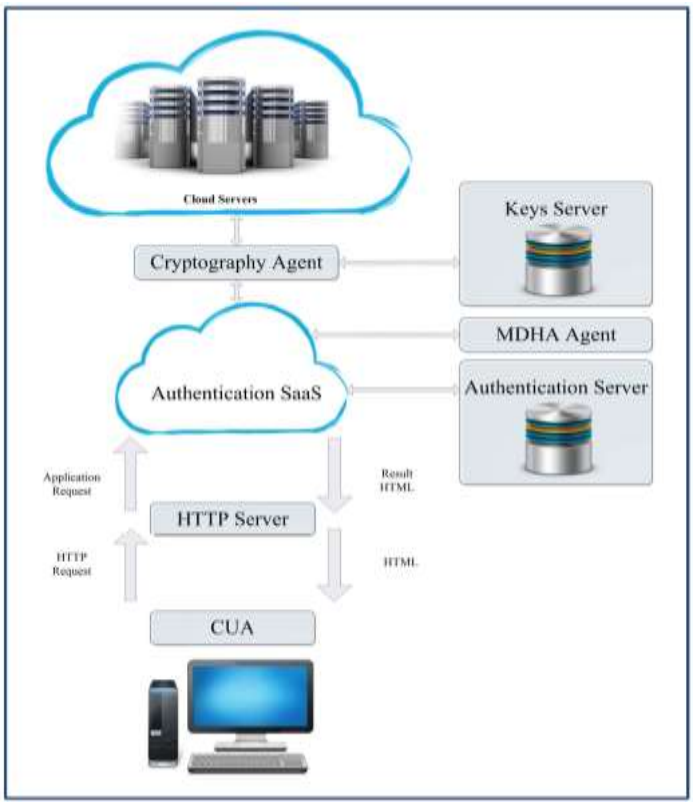
3.2 The Rivest Shamir Adleman or RSA is a cryptosystem for public-key e, and is widely used for securing sensitive data, particularly when being sent over an insecure network . RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts

Institute of Technology. Public-key cryptography also known Asymetric, uses two different but mathematically linked like one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.

3.3 In literature survey, **Modified Diffie-Hellman algorithm** was published by Whitefield Diffie & Martin Hellman in 1976 for password based authentication and key exchange protocol[1].This protocol is work in three phases. Initialization, Registration and Authentication. Diffie Hellman is an algorithm used to establish a shared secret key between two parties. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES. The algorithm in itself is very simple. It is used to secure a variety of internet services. [5]

4. PROPOSED MODEL

In proposed model scheme to access the data from cloud there are separate authentication server will be provided as that only for the authentication purpose so that it will verify and separate authenticate user from non-authenticated user so that only legitimate user can get service from cloud server. In this architecture we are also provide the access control to different user according to their access privilege so that user can access only that data for which user having privilege for that data. CUA and MDA were defined as two main agents for the suggested model. However, for achieving more efficiency and scalability in the process of accessing to cloud-based environments, other tools and techniques should be defined. Figure 1 shows the proposed scheme in general.



1. Client Based User Authentication and Modified Diffie Hellman Authentication were defined as two main agents for the suggested model. However, for achieving more efficiency and scalability in the process of accessing to cloud-based environments, other tools and techniques should be defined. Figure 1 shows the proposed scheme in general.

2. According to the model, authentication process has been separated from cloud servers and performed by a Software-asa- Service application. Authentication SaaS (ASaaS) was defined to decrease the dependency of establishing security in authentication process from security of data in cloud servers.

3. Furthermore, CUA and MDHA communicate with ASaaS instead of the mail cloud servers. Accordingly, the details of these agents such as unique codes, passwords, logs, and mathematical exponents are stored in a separate server that is named Authentication Server (A-Server).

4. In addition, Cryptography Agent (CGA) was defined to encrypt data before storing in cloud servers. This encryption will be done by HE-RSA algorithm [4] by using dual encryption and 2 different decryption keys based on RSA algorithm for enhancing the security in cloud servers. Proposed [5] [12]. Proposed MDHA is used to provide mutual authentication which interacts with software-as-a-service application (ASaaS) instead of actual cloud server. It reduces the load of providing security in authentication process on cloud servers.

6. 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. therefore, a client-based user authentication agent was introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a service application was used to confirm the process of authentication for un-registered devices.

7. REFERENCES

1. Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi,Shirin Dabbaghi Varnos faderani “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments” 2014 IEEE Region 10 Symposium 978-1-4799-2027-3 ©2014 IEEE.

2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. 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.

3. H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, —Dual RSA and Its Security Analysis, IEEE Trans. on Information Theory, vol. 53, no. 8, pp. 2922-2933, August 2007.

4. Sandeep Saxena, Goutam Sanyal, Shashank Srivastava, “Mutual Authentication Protocol Using Identity Based Shared Secret Key in Cloud EnvironMents,” IEEE International Conference on Recent Advances and Innovations in Engineering, Jaipur, May 2014, pp. 1-6.

5. Raphael C.-W. Phan, *Fixing the integrated Diffie-Hellman-DSA key exchange protocol.”* VOL. 9, NO. 6, IEEE JUNE.

6. F. Fatemi Moghaddam, N. Memari, A. Hakemi, and H. Latifi, “A Reliable E-Service Framework based on Cloud Computing Concepts for SaaS Applications,” in *Proc. IEEE Conference on e-*

Learning, e-Management and e-Services (IC3e), Sarawak, Malaysia, December 2013, pp. 100–104.

7. A. J. Choudhury, P. Kumar, M. Sain, L. Hyotaek, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in *Proc. IEEE Asia-Pacific Services Computing Conference (APSCC)*, Jeju Island, South Korea, 2011, pp.110-115.

8. D. Boneh and G. Durfee, —Cryptanalysis of RSA with private key d less than N0.292,‖ *IEEE Trans. on Information Theory*, vol. 46, no. 4, pp. 1339-1349, July 2000.

9. C. Tien-Ho, Y. Hsiu-lien, and S. Wei-Kuan, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," in *Proc. 5th FTRA International Conference Multimedia and Ubiquitous Engineering (MUE)*, Loutraki, Greece, 2011, pp.155- 159.

10. L. B. Jivanadham, A.K.M.M Islam, Y. Katayama, S. Komaki, and S. Baharun, "Cloud Cognitive Authenticator (CCA): A Public Cloud Computing Authentication Mechanism," in *Proc. International Conference on Informatics, Electronics & Vision (ICIEV)*, Dhaka, Bangladesh, 2013, pp. 1-6.

11. W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (1976) 644–654.

12. T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans.*Inform. Theory 31 (1985) 469–472.