Secure Mutual Authentication for Cloud Environment

Shipra Kataria
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India

Rupali Syal
Department of Computer Science and Engineering
PEC University of Technology
Chandigarh, India

Abstract— **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 ASaaS 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. According to the analysis of the proposed scheme, it is resistant from many attacks like Man in the Middle attack.**

Keywords: Cloud computing; authentication; cryptography; encryption

I. INTRODUCTION

Cloud computing is a growing technology which is based on various concepts like storage, virtualization, processing power. It allows customers to save their data with a cloud server and to gain services anytime and anywhere. Cloud computing provides services for a large domain: from computing power to computing infrastructure and from business to personal collaboration. It provides us many services like Software-as-a-service (SaaS), Platform-as-a-service (PaaS), Infrastructure-as-a-service (IaaS), Database-as-a-service (DaaS) and many more services [1] [2]. There are many advantages of migrating data to cloud side since the user can store unlimited data on cloud and can access the data from cloud on his demand using any device without taking care of the cost of software and hardware infrastructure.

However, security has become the most sensitive issue in cloud computing environments.[3] Cloud computing brings many security challenges. The security has been divided to several parts and one of the most important parts is ensuring authentication while storing data on cloud. Vulnerabilities present in an authentication scheme leads to many security breaches which allow an intruder to access the cloud resources [4]. Many schemes have been implemented in literature regarding user authentication in cloud [5]-[8]. It has been also suggested in the previous schemes that mutual authentication between server and user should be done to prevent various attacks like man in the middle attack. This challenge motivates to propose a secure mutual authentication model which authenticates both the server and the user so that both parties can securely exchange data on cloud. The proposed scheme consists of four phases such as Connection Establishment, Registration, Login, Authentication.

The rest of the paper is organized as follows. Section 2 consists of related work. Section 3 presents the proposed mutual authentication model for cloud environments. Section 4 discusses the evaluation of proposed model. Finally Section 5 presents conclusion and future work.

II. RELATED WORK

To prevent impersonation attacks on cloud environment various authentication schemes have been proposed in literature.

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]. The main benefit of this scheme is that the authentication process is separated from cloud servers and performed by a software-as-a-service application. According to the evaluation, the proposed scheme can resist considerable attacks like man-in-the middle attack, timing attack, brute force attack etc.

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. The model provides mutual authentication with the help of signature and identity. According to analysis of performance, this scheme improves the computational and communicational efficiency.

A strong user authentication framework for cloud computing was proposed by Amlan Jyoti Choudhury et al. in 2011 [8] in which user legitimacy is strongly verified before entering into cloud by providing mutual authentication, session key establishment, identity management between users and cloud server. The proposed scheme uses two-step verification based on password, smartcard and out of band authentication to verify user authenticity. According to the evaluation, the suggested framework resists various attacks like replay attack, denial of 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.

Many authentication schemes exist in literature. Some prevent Man in the Middle attack while some provide only user authentication. It has been suggested in [5] that there should be mutual authentication between user and server that prevents Man in the Middle attack. The proposed scheme provides secure mutual authentication in cloud computing environments.

III. PROPOSED SCHEME

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 handled by Authentication Software-as-a service (ASaaS) application. This reduces the load on cloud servers [5]. The notations used in this work are summarized below in TABLE 1.

TABLE I. NOTATIONS

IDa	User's Identity
PWa	User's Password
Upb	User's public key
Upr	User's private key
Spb	Server's public key
Spr	Server's private key
X	X co ordinate of server's public key
Y	Y co ordinate of server's public key

The scheme consists of four phases: connection establishment, registration phase, login phase and authentication phase.

A. Connection establishment

The initial connection between client and server is created with the help of HTTPS and SSL protocols [10] After the connection is established, the public keys of client and MDHA server are exchanged. The key generation is done by using Elliptic Curve Cryptography algorithm [11].

B. Registration phase

In this phase, user needs to register himself at the server by providing his identification details. The procedure is as follows:

- The user Ua selects IDa and PWa and sends it to MDHA over a communication channel by encrypting it with the server's public key exchanged during connection establishment.
- When MDHA receives the registration request, it decrypts the IDa and PWa by using its own private key . The received ID is checked with the existing IDs in user database. If both are equal, MDHA rejects the registration request otherwise stores the identification details of new user in the database of cloud.

C. Login Phase

When the user wants to login into the cloud environment, this phase is invoked. In this users are verified before accessing the cloud. The procedure is as follows:

- User enters IDa, PWa and send it to MDHA over the public channel by encrypting them using server's public key so that no intruder can get ID and password. A random message R is also sent along with the login credentials which acts as a token for server authentication.
- After getting login request, MDHA decrypts the request by using its own private key. MDHA matches the login credentials with the credentials saved in the database during registration phase. If both are same, then the login status is approved otherwise rejects the login request.
- MDHA calculates R_1 and sends it to user along with the random message sent by the user. The messages are encrypted with the public key of user. If the user gets the same random message from MDHA after decryption, it proves that MDHA is the actual server that sent the message.

D. Authentication phase

This phase proves user authentication. User calculates R_2 on its own side and also calculates E by using R_1 sent by MDHA. The R_2 is encrypted by E. User sends the E and R_2 to MDHA server by encrypting with server's public key. MDHA decrypts the message using its own private key and calculates a key E on its own side by using R_2 sent by user and uses this key to decrypt K. After decryption if both R_3 and R_2 matches, the user is authenticated. In this way mutual authentication takes place and no unauthorized person can get access to the services of cloud.

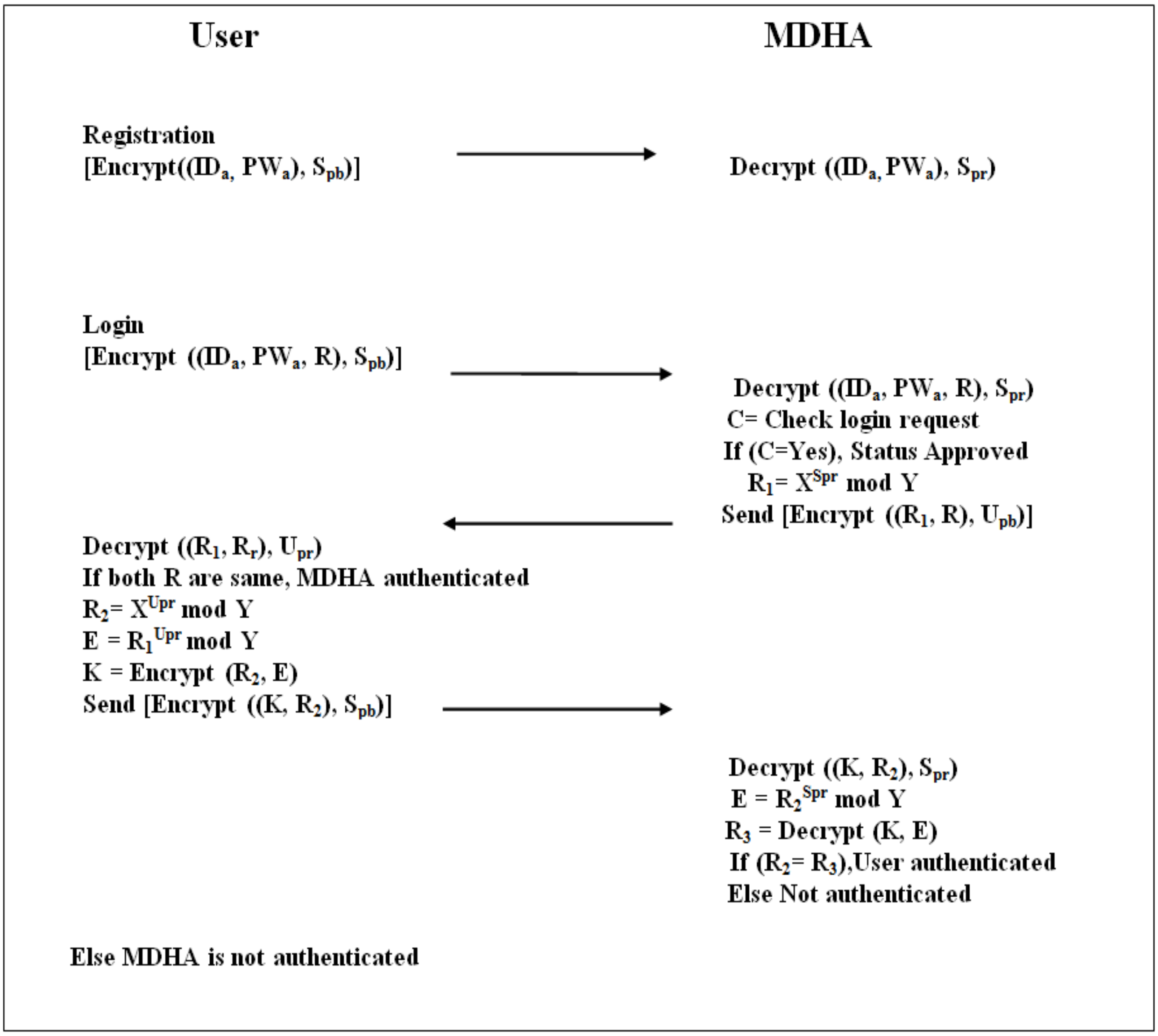
User
MDHA
Registration
[Encrypt((ID_a, PW_a), S_{pb})]
Decrypt ((ID_a, PW_a), S_{pr})
Login
[Encrypt ((ID_a, PW_a, R), S_{pb})]
Decrypt ((ID_a, PW_a, R), S_{pr})
C= Check login request
If (C=Yes), Status Approved
R_1= X^{Spr} mod Y
Send [Encrypt ((R_1, R), U_{pb})]
Decrypt ((R_1, R_r), U_{pr})
If both R are same, MDHA authenticated
R_2= X^{Upr} mod Y
E = R_1^{Upr} mod Y
K = Encrypt (R_2, E)
Send [Encrypt ((K, R_2), S_{pb})]
Decrypt ((K, R_2), S_{pr})
E = R_2^{Spr} mod Y
R_3 = Decrypt (K, E)
If (R_2= R_3),User authenticated
Else Not authenticated
Else MDHA is not authenticated

Fig 1 : Mutual Authentication Algorithm

Proposed Modified Diffie Hellmann algorithm provides more security than Modified Diffie Hellmann algorithm as MDHA provides user authentication only and does not prevent Man in the Middle attack from server side while proposed MDHA prevents this attack by providing secure mutual authentication through encrypted communication between user and server [5] [12]. Fig. 1 shows the communication between user and server in proposed secure mutual authentication algorithm in cloud environment. The sensitive data is encrypted which increases the overhead but provides secure and confidential communication

Fig.2 shows the proposed model for authentication in cloud. 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. In addition to MDHA, there is another agent called cryptographic agent encrypts the data before uploading on cloud. The idea of a separate authentication server and encryption server is also expressed in [5]. The key generation and encryption is performed by Elliptic Curve Cryptography (ECC) algorithm or enhancing security in cloud servers. The advantages of ECC is its smaller key size and it has sub exponential time complexity property which makes it difficult to crack [13] [14]. Also the elliptic curve discrete logarithmic property of ECC provides faster computation than other discrete logarithm. [15]

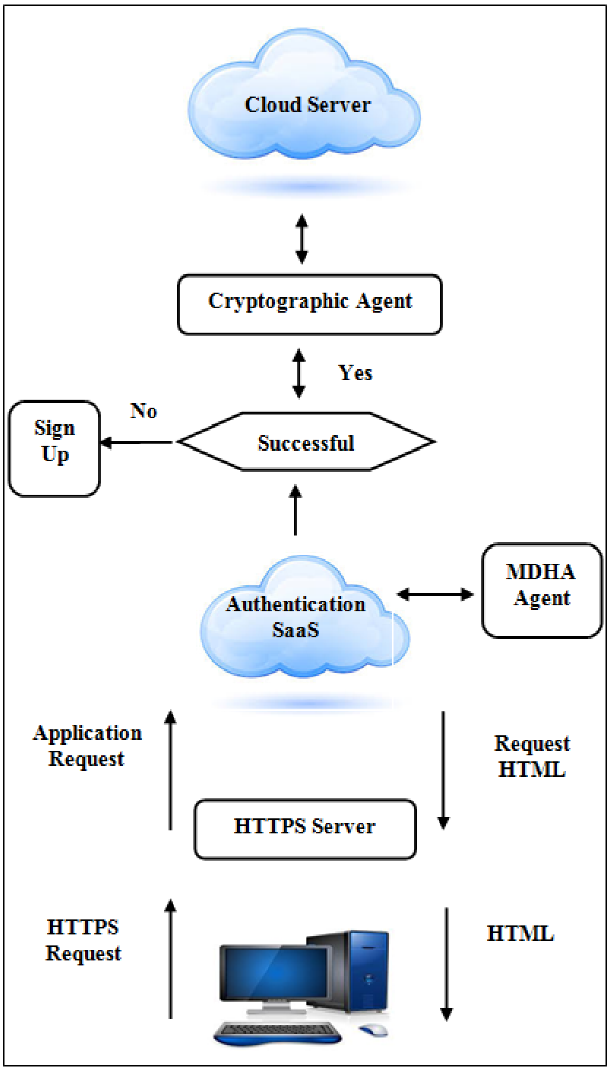

Fig.2. Proposed Model

IV. Evaluation of Proposed Scheme

This section presents the analysis of proposed scheme.

1) Mutual authentication: Mutual authentication provided in proposed model prevents an adversary to impersonate a legal user to MDHA agent and vice versa. It is done by two factors:first factor is the random message sent along with the login credentials which proves MDHA's authenticity and the other is encrypted R_2 sent along with original R_2 which proves user authenticity. In this way mutual authentication is performed.

2) *Complexity:* The proposed scheme reduces the time complexity as there is no need to find large random prime numbers for authentication algorithm. The modified Diffie Hellmann algorithm is performed by taking x and y co ordinates of MDHA's public key which is generated during connection establishment.

3) Security: The proposed scheme is resistant from many attacks.

a) Man in the Middle attack: The proposed model is resistant from Man in the Middle attack because of the encrypted replies R1 and R2 and mutual authentication between MDHA and the user. The random message R sent by user acts as a token for server authentication and prevents this attack from server side. User authentication is provided by comparing R2 and R3. If E_{MDHA} is not equal to E_{user} , the man in the middle attack can be easily identified and can be prevented.

b) *Phishing attack:* Mutual authentication provided in this scheme prevents phishing attack as only the actual user and server can send the identification data to each other which is verified by the other party. In this way no unauthorized person on the cloud server can acquire sensitive information.

c) Resistance to Masquerade attack: In order to behave as legitimate user, an attacker must forge a valid login request so that server can pass the authentication process. To perform this task, login request sent by actual user must be decrypted which becomes difficult for an attacker. Unless an attacker obtains actual decryption keys, he can not forge the valid login request. Therefore, this scheme is resistant from masquerade attack.

V. Conclusion and future scope

A model for secure mutual authentication for cloud computing environment has been proposed. Modified Diffie Hellmann algorithm provides mutual authentication between server and user and interacts with ASaaS 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. The future work will be to implement the proposed scheme in cloud simulator cloudsim.

References

[1] 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.

[2] Akhil Behl, Kanika Bhel, “An Analysis of Cloud Computing Security Issues”, World Congress on Information and Communication Technologies, IEEE, 2012, pp. 109-114.

[3] Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI, “Cloud computing : security challenges”, IEEE, 2012, pp. 26-31.

[4] Jaidhar C. D, “Enhanced Mutual Authentication Scheme for Cloud Architecture,” IEEE 3rd International Advance Computing Conference, Ghaziabad, February 2013, pp. 70-75.

[5] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh,Sagheb Kohpayeh Araghi, Nima Morad Alibeig, Shirin Dabbaghi Varnos-faderani, “A Scalable and Efficient User Authentication Scheme for CloudComputing Environments,” IEEE Region 10 Symposium, Malaysia,, April 2014, pp. 508-516.

[6] Vishal Paranjape, Vimmi Pandey, “An Improved Authentication Technique with OTP in Cloud Computing,” International Journal of Scientific Research in Computer Science and Engineering, vol 1, pp. 22-26, 2013.

[7] Ganesh V.Gujar, Shubhangi Sapkal, Mahesh V.Korade, “STEP-2 User Authentication for Cloud Computing,” International Journal of Engineering and Innovative Technology, vol. 2, pp. 106-109, April 2013.

[8] Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee, “A Strong User Authentication Framework for Cloud Computing,” IEEE Asia -Pacific Services Computing Conference, pp. 110-115, Jeju Island, December 2011, pp. 110 - 115.

[9] Sanjeet Kumar Nayak, Subasish Mohapatra, Banshidhar Majhi, “An Improved Mutual Authentication Framework for Cloud Computing,” International Journal of Computer Applications, vol. 52, pp. 36-41, August 2012.

[10] Neha Tirthani, Ganesan R, “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography,” IACR Cryptology ePrint Archive, 2014.

[11] Ms. A A Deshmukh, Ms. Manali Dubal, Dr. Mahesh TR, Mr. C R Chauha, “Data Security Analysis And Security Extension For Smart Cards Using Java Card, ” International Journal of Advanced Information Technology, vol. 2, pp. 41-57, April 2012.

[12] G. R. Kumar, F. Zeeshan, and M. Shahabuddin, “Discovering Man-in-the-Middle Attacks in Authentication Protocols,” IEEE Military Communications Conference, Orlando USA, October 2007, pp. 1-7.

[13] M. Muni Babu, S. MP. Qubeb, V. Sunil Babu, “A Comparative Study Of Elliptic Curve Cryptography and RSA to KERBEROS Authentication Protocol,” International Journal of Advances in Science Engineering and Technology, vol. 1, pp. 43-45, January 2014.

[14] Bhavana Sharma, “Security Architecture of Cloud Computing Based on Elliptic Curve Cryptography (ECC),” 2nd International Conference on Emerging Trends in Engineering and Management, vol. 3, July 2013, pp. 58-61.

[15] Ching-Nung Yang, Jia-Bin Lai, “Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing,” International Symposium on Biometrics and Security Technologies, IEEE, Chengdu, July 2013, pp. 259-266.