A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments

[1]Faraz Fatemi Moghaddam
Faculty of Computer Science and IT
U.P.M. University
Selangor, Malaysia
f.fatemi@ieee.org

[2]Shiva Gerayeli Moghaddam
Faculty of Computing
U.T.M. University
Johor, Malaysia
shivagerayeli20@gmail.com

[3]Sohrab Rouzbeh
Collage of Information Technology
University Tenaga National
Kajang, Malaysia
sohrab.rouzbeh@gmail.com

[4]Sagheb Kohpayeh Araghi
Faculty of Engineering
M.M.U. University
Cyberjaya, Malaysia
1081600074@student.mmu.edu.my

[5]Nima Morad Alibeigi
Faculty of Built Environment
Heriot-Watt University
Edinburgh, UK
nm373@hw.ac.uk

[6]Shirin Dabbaghi Varnosfaderani
Faculty of Computer Science and IT
U.P.M. University
Selangor, Malaysia
shirindabaghi@gmail.com

***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. 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. Furthermore, a cloud-based software-as-a-service application has been used to confirm the process of authentication for un-registered devices. Moreover, there are two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In overall, the theoretical analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments as an emerging and powerful technology in various industries.**

Keywords—Cloud Computing; User Authentication; Scalability; Agent; Cryptography;

I. INTRODUCTION

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 [1]. There are many concepts that have been used in cloud-based services (*i.e.* virtualization, storage, processing power, connectivity, and sharing) 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 [2]. 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. This security has been divided to several parts and one of the most important parts is ensuring about the user authentication processes [4] and managing accesses when users outsource sensitive data share on public or private cloud servers [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. Furthermore, controlling the simultaneous accesses and operations in shared files is the other challenge during user authentication when the number of end-users is increased. In fact, it can be concluded that many challenges will be grown in user authentication and managing accesses when the rate of cloud services subscribers is raised. Therefore, a scalable user authentication algorithm has been proposed in this paper and the suggested model has been justified and evaluated respectively.

II. RELATED WORKS

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 [6]. In this part, some of the related user authentication models have been reviewed.

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.

OpenID authentication [8] was a cloud-based platform independent, scalable, flexible, and decentralized authentication model that was introduced in IEEE IAS 2011. Improving usability and seamless Single Sign On (SSO) experience for the users are the major benefits of this model that was established for front-end GUI servers, and performs the authentication in the back-end at a single policy decision point and let end-users to use unique OpenID identifiers from OpenTD providers.

A dynamic ID-Based remote mutual authentication model [9] based on Elliptic Curve Cryptosystem (ECC) was proposed in 2011. Furthermore, cloud Cognitive Authenticator (CCA) is integrated authentication model [10] that was proposed in 2013. CCA uses the concepts of one round Zero Knowledge Proof (ZKP) and Advance Encryption Standard (AES) to enhance the security in public, private or hybrid clouds by four procedures providing with two levels of authentication and encrypting the user identifiers. The main specification of CCA in comparison with other models is the coverage of the two levels of authentication together with strength of the encryption algorithm. However, interoperability and compatibility with AES are the major weaknesses of CCA.

There are many other user authentication schemas that have been accessible in [11]-[16] for further researches. Lacks of scalability, efficiency, compatibility or correctness are the main disadvantages of these algorithms than have decreased the reliability in cloud computing environments. The proposed model tries to use the strengths of each model and eliminate weaknesses to provide an efficient, scalable, and reliable user authentication in cloud-based services.

III. Proposed Model Tools

According to literature, lack of trust, efficiency, and scalability in user authentication and access processes are challenging issues in cloud-based environments. Therefore, an efficient and scalable user authentication algorithm has been proposed in this paper and evaluated according to defined parameters. The proposed model was designed by using concepts of agent [17]-[18] and following tools:

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 [19] algorithm. In client-side, user will decrypt the unique access code and set the decrypted code on the installed extension. By this extension, a part of user authentication process will be done in client side and the dependency of this process on service providers will be reduced significantly. The algorithm of client-based user authentication has been shown in table 1.

TABLE I: ALGORITHM OF CLIENT-BASED USER AUTHENTICATION

Client		**Server**
	Registration of Device and Installation of Extension	
Registration-Request (Com ID, Mac ID, User ID, Access Type*)	→	R = *Check-the-Request* (Com ID, Mac ID, User ID, Access Type*)
	←	*If (*R=yes*) then Confirm-Request* ( )
Send-Optional-Password (PW)	→	
		ACG = *Access-Code Generation* ( ) DL = *Download-Link-Generation* ( ) EACG = *Encrypting* (ACG, PW)
	←	*Send* (DL, EACG)
Download-Extension (DL) ACG = *Decrypting* (EACG, PW) *Install-Extension* (ACG)		
	Access to Cloud-Based Service Provider	
Open-Web-Browser ( ) *Enter-Password* (PW) *Check-Password* (ACG, PW) *Confirm-Access* ( )	→	

* Access type can be temporary, provisional or permanent according to user's request.

TABLE II: ALGORITHM OF MODIFIED DIFFIE-HELLMAN AGENT USER AUTHENTICATION

Client		MDHA Agent
User Authentication with an Un-Registered Device		
Login (Username, Password)	→	L = *Check-the-Login-Request* (Username, Password) *If* (L=yes) *then* Login-Statues = *Approved* *Define* (Large Random Prime, P) *Define* (Large Random Prime, G) *Define* (Integer, x) $R_1 = G^x$ *mod* P *Send* (P, G, R_1)
	←	
Define (Integer, y) $R_2 = G^y$ *mod* P $K = R_1^y$ *mod* P E = *Encrypt* (R_2, K) *Send* (E, R_2)	→	
		$K = R_2^x$ *mod* P R_3 = *Decrypt* (E, K) *If* (R_2=R_3) *then* Login-Statues = *Confirmed* *else* Login-Statues = *Rejected*

B. *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.

According to the performance of this agent in comparison with original Diffie-Hellman [21], authentication concerns by an un-registered device has been solved by encrypting K before sending to MDHA while the original Diffie-Hallman is not appropriate in this model and has serious weaknesses as it faces Discrete Logarithm attack and Man in the Middle attack [22].

IV. PROPOSED MODEL SCHEME

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.

According to the model, authentication process has been separated from cloud servers and performed by a software-as-a-service application. Authentication SaaS (ASaaS) was defined to decrease the dependency of establishing security in authentication process from security of data in cloud servers. 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 was named Authentication Server (A-Server).

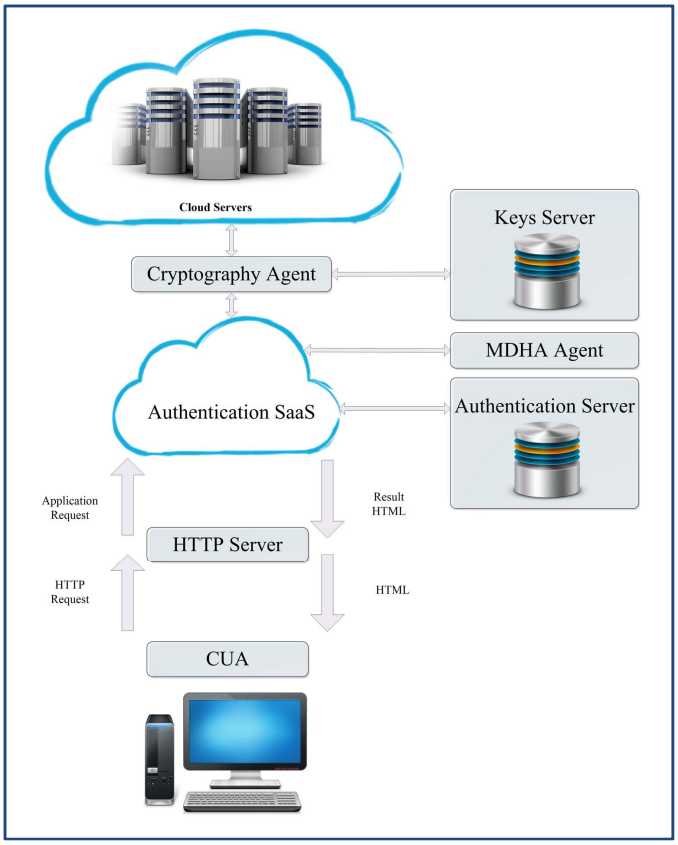

Fig. 1. Proposed Model Scheme

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 [23] for enhancing the security in cloud servers. It should be noted that cryptography details such as keys and logs will be stored in Keys Server (K-Server) and separate from main cloud server. The algorithm of HE-RSA is as follows:

A. Key Generation Algorithm

1. Randomly and secretly choose two large primes: p, q and compute $n = p.q$
2. Compute $\varphi(n) = (p-1)(q-1)$.
3. Compute
$$\gamma(n,h) = (p^h - p^0)(p^h - p^1) \dots (p^h - p^{h-1}) + (q^h - q^0)(q^h - q^1) \dots (q^h - q^{h-1}).$$
4. Select Random Integer: r such as $1 < r < n$ and $\gcd(r, \varphi) = 1$ and $\gcd(r, \gamma) = 1$ (r should be a small integer).
5. Compute e such as $r.e \equiv 1 \; mod \; \varphi(n)$ and $1 < e < \varphi(n)$.
6. Compute d such as $d.e \equiv 1 \; mod \; \gamma(n)$ and $1 < d < \gamma(n)$.
7. Public Key: (e, n).
8. Private Key: (r, d, n).

B. Encryption Process

1. Suppose entity A needs to send message m to entity B (represent m as an integer in the range of $0 < M < n$).
2. Entity B should send his public key to entity A.
3. Entity A will encrypt m as :
$$c = ((m^e mod\ n)^e mod\ n)$$
After that Entity A will send c to entity B.

C. Decryption Process

1. Entity B will decrypt the received message as: $m = ((c^r mod\ n)^d mod\ n)$.

V. Evaluation of Proposed Model

Evaluation process of the proposed model has been done according to following parameters:

A. 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. Furthermore, using a cloud-based and separate authentication software-as-a-service from main cloud servers will increase the ability of managing authentication in large number of requests simultaneously. The point of defined agents is using a specific and separate server for each agent to make the framework more manageable.

B. Effeciency

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. Accordingly, each agent can confirm the identity of user separately but it will be helped by other agent against incomplete or suspicious authentications. In addition, increase the role of users in the process of protecting and accessing to their own data is the other feature of proposed model that increase efficiency and also reliability in cloud computing environment considerably.

C. Security

By using various tools and techniques during authentication and also data protection processes, security of the suggested model has been improved. Establishing 2 types of encryption (*i.e.* AES-256, HE-RSA-2048) during authentication and before storing data in cloud servers will enhance the rate of trust in the framework. Moreover, the proposed model can resist against various attacks as follows:

1) Man in the Middle Attack

To protect the suggested model from Man in the Middle attack, encrypted replies ($R_1 \; and \; R_2$) and mutual authentication between MDHA and end-user is required. For this purpose user computes $K_{User} = R_1^y \bmod G$ and $E = Encrypt(R_2, K_{User})$ and sends R_2, E to MDHA. By this process, MDHA computes $K_{MDHA} = {R_2}^x \bmod G$ and $R_3 = Decrypt(E, K_{MDHA})$. These processes prevent the Man in the Middle attack and by comparing R_2 and R_3 the attack will be identified. According to this comparison, R_2 and R_3 are not same for MDHA because the keys between users and attackers are different.

$$K_{MDHA} = P^{xz} \bmod G$$
$$K_{User} = P^{yz} \bmod G$$
$$K_{Attacker} = P^{yz} \bmod G$$

It means $K_{MDHA} \neq K_{User} = K_{Attacker}$ and because of that, the Man in the Middle attack was noticed by MDHA and the attack was prevented.

2) Brute Force Attack

All possible combinations to guess the private key have been tried by the attacker during the brute force attack. Using HE-RSA in the proposed model makes this algorithm has significant resist against brute force attack by 1024 bits of exponent size whereas, the original RSA need 2048 exponent size to resist against this attack [24].

3) Timming Attack

Timing attack is a side channel attack, in which the attacker determines private exponent by calculating the time with exploiting the timing variation of the modular exponentiation [25]. Dual encryption in HE-RSA before storing data to cloud servers will protect data from this attack and it's not required to multiply data to prevent this attack.

VI. RECOMMENDATIONS

Due to a separate cryptography server from main servers [26] in proposed framework, it is suggested to use a smart data header during access control processes for helping to handle possible error better and more significant. The notations of data headers will save log data for increasing the efficiency of error identification and error handling during access control processes.

VII. CONCLUSION

According to the challenging issues during the user authentication and access control process in cloud-based environments, an efficient and scalable user authentication scheme was proposed in this paper. 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. Furthermore, a cloud-based software-as-a-service application was used to confirm the process of authentication for un-registered devices.

Moreover, there are two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In overall, the theoretical analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments as an emerging and powerful technology in various industries.

ACKNOWLEDGMENT

We acknowledge the assistance and logistical support provided by University Putra Malaysia (U.P.M.), Meta Soft Company, Dr. Pardis Najafi, Ms. Fatemeh Afsahi, Er. Hamid Gerayeli, Ms. Sori Saburi Rad, and the bright memory of Dr. Enayat Fatemi Moghaddam.

REFERENCES

[1] 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.

[2] F. Fatemi Moghaddam, *Secure Cloud Computing with Client-Based Control System: Protection of Stored Cloud-Based Data by Increasing End-User's Role*, Chapter 1: Cloud Computing, 1st Edition. Saarbrücken: Lambert Academic Publishing (LAP), 2013, pp. 9-2.

[3] D.G. Chandra, and R.S. Bhadoria, "Cloud Computing Model for National E-governance Plan (NeGP)," in *Proc. 4th International Conf. on Computational Intelligence and Communication Networks (CICN)*, Mathura, 2012, pp. 520-524.

[4] F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments," *Journal of Advances in Computer Networks*, vol. 1, no. 3, pp. 238–241, 2013.

[5] 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

[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] R.H. Khan, J. Ylitalo, and A.S. Ahmed, "OpenID Authentication as a Service in OpenStack," in *Proc. 7th International Conference on Information Assurance and Security (IAS)*, Melaka, Malaysia, 2011, pp. 372-377.

[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] M.K. Khan, "Cryptanalysis and Security Enhancement of Two Password Authentication Schemes with Smart Cards", in *Proc. IEEE International Multi-topic Conference (INMIC)*, Lahore, Pakistan, 2007, pp. 1-4.

[12] I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "A Password Authentication Scheme over Insecure Networks," *Journal of Computer System*, vol. 72, no. 4, pp. 727-740, 2006.

[13] E.J. Yoon, and K.Y. Yoo, "New Authentication Scheme based on a one-way Hash Function and Diffie–Hellman Key Exchange," *Cryptology and Network Security Lecture Notes in Computer Science*, vol. 3810, Springer-Verlag, pp. 147-160, 2005.

[14] M. Scott, "Cryptanalysis of an Id-Based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM SIGOPS Operating Systems Review*, vol. 38, no. 2, pp. 73-75, April 2004

[15] B. Wang, J.H. Li, and Z.P. Tong, "Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme," *Elsevier Journal of Computers & Security*, vol. 22, no. 7, pp. 643-645, October 2003.

[16] G.Yang, D. S. Wong, H. Wang, and X. Deng, "Two-Factor Mutual Authentication based on Smart Cards and Passwords", *Journal of Computer and System Sciences*, vol. 74, pp. 1160-1172, 2008.

[17] F. Q. Zhang, and D. Y. Han, "Applying Agents to the Data Security in Cloud Computing," in *Proc International Conf. on Computer Science and Information Processing (CSIP)*, Shaanxi, China, 2012, pp. 1126-1128.

[18] M. Hajivali, F. Fatemi Moghaddam, M. T. Alrashdan, and A. Alothmani, "Apply an Agent-Based User Authentication and Access Control Model for Cloud Servers," in *Proc. IEEE International Conference on ICT Convergence*, Jeju Island, South Korea, October 2013, Pages: 807-812.

[19] J. Daemen, and V. Rijmen, "AES Proposal: Rijndael". *National Institute of Standards and Technology*, p. 1-10. Apr 2001.

[20] M. K. Ibrahem, "Modification of Diffie-Hellman Key Exchange Algorithm for Zero Knowledge Proof," in *Proc. International Conf. on Future Communication Networks (ICFCN),* Baghdad, Iraq, 2012, pp. 147-152.

[21] W. Diffie, and M. Hellman, "New directions in cryptography," *IEEE Trans. on Information Theory*, vol. 22, pp. 644–654, 1976.

[22] G. R. Kumar, F. Zeeshan, and M. Shahabuddin, "Discovering Man-in-the-Middle Attacks in Authentication Protocols," in *Proc. IEEE Military Communications Conf. (MILCOM),* Orlando, USA, 2007, pp. 1-7.

[23] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *ACM Trans. On Communications*, vol. 21, pp. 120-126, 1978.

[24] A. Alhasib, and A .M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," in *Proc. 3rd International Conference on Convergence and Hybrid Information Technology (ICCIT)*, Busan, 2008, pp. 505-510.

[25] Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Proc. 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'96)*, London, 1996, pp. 104-113.

[26] F. Fatemi Moghaddam, O. Karimi, and M. T. Alrashdan, "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, Pages: 185-189.