Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Authentication Scheme in Cloud Computing Environment

Palak Raina and Bhavik Patel
Computer Science and Engineering
Institute of Technology, Nirma University
Ahmedabad, Gujarat 382481, India

Abstract: Cloud computing could be a paradigm of rising technology, providing the variety of services over the web. With the additional advancement and with an advent of recent techniques, security is motility a threat to the present technology. Several authentication schemes are framed over the years to supply security. With additional technologies, the number of attacks has conjointly been terrible. The basic parole primarily based authentication, theme doesn't offer abundant security for information in the cloud setting. So, a powerful authentication, theme is needed. In this paper, a study of ascendable and economical, user authentication, theme has been done. During this theme, the user entry is powerfully verified before being given entry to a cloud. This is often done by the theme of victimization the construct of an agent. In recommended model, to substantiate the identity of a user, consuming primarily based authentication agent is employed and for unregistered devices, software package as a service application has been used. To cut back the dependency of authentication and cryptography from main servers, separate servers are used for various processes.This provides additional reliable and secure system. Analysis of this recommended theme shows that the projected model can bring additional reliability, efficiency and full user trust in victimization cloud computing services and can bring additional security in cloud computing setting.

Keywords: Cloud Computing, User Authentication, SaaS, Cryptography

I. INTRODUCTION

Cloud Computing could be a model for providing a pool of resources, On demand access to multiple Computing services.[1] This model has heaps of benefits as everyone will get access to totally different resources anytime, anywhere. The distinct model of Cloud: SaasS (Software As A Service) ,PaaS(Software As A Service) and IaaS (Infrastructure as a Service) provides users with access of application softwares, databases, development tools on demand basis. These have varied blessings like providing unlimited storage [2] .Moreover, Throughout property,easy and reliable access square measure the opposite edges [3].By providing these services over the web, it eradicates the requirement of putting in and running the applications on the users own Computers and users get quicker and easier access to their knowledge from any location.

Cloud services, suppliers provide several services to users, however security plays a serious role in cloud environments. Many challenges are involved in moving data to cloud and maintaining it over cloud data centers.Use all resources are accessed via the internet even if the cloud provider focuses on security in the cloud infrastructure, the data will be transmitted to the users through the network, which may be insecure [4]. In this paper, authentication scheme is analyzed that strengthens the security of cloud environments.There are two main phases involved in this scheme, that is, Registration phase, in which users are identified and the other phase is a service operation phase in which users are authenticated and their access control privileges are acquired. Therefore,a very scalable

Authentication scheme is proposed in this paper and suggested model is analyzed over various security threats that will show the strength of this authentication scheme.

II. LITERATURE SURVEY

Before discussing our planned model, let's review some connected models that were planned before. One in every of the foremost standard user authentication, theme was steered by Lamport [5] in 1981, in which, users watchword was hold on as hash price in the server. During this theme, table was maintained to verify the watchword and verify the legitimacy of users the downside with this theme was that if watchword table taken, or changed, then the system might be simply compromised .After this some open-end credit based mostly watchword authentication schemes were planned [6][7] . Later In 2010, Kamara and Luther [8] did work on public cloud infra-structure. Afterwards, Popa et al. [9] Presents Cloud Proof, a secure storage system that steered to extend security over the cloud. During this model, users will notice violations of confidentiality, integrity. The model uses scientific discipline tools combined with engineering efforts to get an associate degree economical and climbable system that helped in police investigation and proving cloud acts Reus.

In 2011, a robust, user authentication framework for cloud computing was planned by Choudhury et al. Wherever users genuineness is verified before moving into the cloud. It provides Identity management, mutual authentication that's authentication from consumer still as a server, and conjointly session

The key institution between consumer and server [10]. There square measure several alternative themes that were planned, however the problem with all schemes is expeditious, measurability. And with correctness of the theme. The planned

model tries to require the strength of every model and at constant time, eliminating the weak and downsides of antecedently planned models.

III. PROPOSED MODEL STRUCTURE

As studied from previous works, challenges of cloud computing environments embody largely believability and security. So here a versatile client validation algorithmic program has been arranged and assessed on the assurance parameters. The model is predicated on operator thought [11] [12] and is given as taking over:

A. Client-Based User Authentication Agent

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 ( )	→	

C

ustomer based client verification specialist that is placed on end-clients application to confirm the character of client before getting two servers bearing on a cloud. Inside a similar technique, the client got the opportunity to enroll gadgets on administration provider so exchange expansion with its unmistakable get to the code that may encourage inputting in on the application. That particular code is also encoded by an arcanum that has been picked by client exploitation AES algorithmic program. [13]. In customer side, the client can then decode the unmistakable get to code and along these lines offer the unscrambled code on the put in an expansion. By this augmentation, the client verification technique is depleted shopper aspect, and in this manner the reliance is decreased on administration providers. The algorithmic program of customer based client confirmation has been appeared in table one.

B. Authentication based on Modified Deffie-Hellman Agent(MDHA)

Client primarily based user authentication agent is employed for authenticating registered devices. For un-registered de-vices, MDHA theme is employed.This scheme will increase

The dependability in method of authentication for international organization registered devices. Table II shows the algorithmic program of identical. Reliable with the execution of this specialist as contrasted and unique Diffie-Hellman [14], confirmation concern has been settled in Associate in Nursing un-enrolled gadget by encoding K before bringing on to MDHA while its unique Diffie-Hallman is utilized in situ of MDHA it may have genuine effects and shortcoming since it experiences fluctuated dangers and security assaults. [15]

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)
		$R_1 = G^x \bmod P$
	←	*Send* (P, G, R_1)
Define (Integer, y)		
$R_2 = G^y \bmod P$		
$K = R_1^y \bmod P$		
E = *Encrypt* (R_2, K)		
Send (E, R_2)	→	
		$K = R_2^x \bmod P$
		R_3 = *Decrypt* (E, K)
		If (R_2=R_3) *then* Login-Statues = *Confirmed*
		else Login-Statues = *Rejected*

IV. SCHEME OF PROPOSED MODEL

As mentioned higher than, 2 agents in planning model square measure CUA and MDHA. However to attain a lot of measurability and potency, there square measure different tools that are also—also square measure—are needed that are well illustrated in figure one. With regards to this topic, abuse programming as -a-benefit application, Confirmation technique has been isolated for cloud servers. The point of Authentication SaaS (ASaaS) was to diminish the reliance on making security in verification strategy for the security of data on cloud servers. Besides, CUA and MDHA speak with Authentication SaaS as opposed to the mail cloud servers. In this manner, the little print of those operators like particular codes, passwords, logs, and numerical types square measure along these lines hang on in an exceedingly isolate server that was named Authentication Server (A-Server).

Notwithstanding the current, a separate specialist alluded to as Cryptography Agent (CGA) was laid out to encode data before putting away in cloud servers. This cryptography made by HE-RSA administers [16] by abuse twin coding and several totally unique mystery composing keys bolstered RSA algorithmic lead [17] which will upgrade the security in cloud servers. The most element to be noted here is that cryptography points of interest like keys and logs hang on in a few Keys Server (K-Server) that is isolated from the principle cloud server. The algorithmic control of HE-RSA is said in Fig 2:

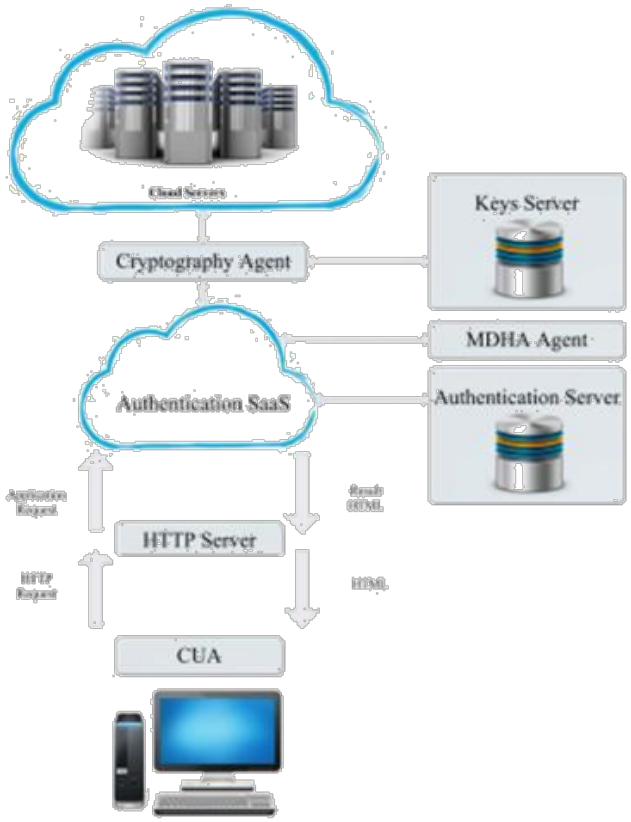

Fig. 1. Model Scheme

V. RESULTS

A. *Performance*

The authentication is completed supported fully, completely different agents for registered additional as for coalition registered devices. in addition thereto, Authentication SaaS must be used that may increase security and reduces the dependency.

B. *Key Generation Time*

The key era time was tried per the RSA Small-e recipe that was set up and by driving the span of keys between 128 bits to 8192 bits. Figure 3 demonstrates the impacts of settling key size in key era time in points of interest: per the outcomes, the expansion of era time in the Effects of settling key size RSA little e is 23 PC however Original RSA. Encourage progressively and as an aftereffect of check of UAA1 in regards to the affiliation, 1024 bits of key size is that the first pertinent key size for exploitation in SUAS. In addition, this size was picked as a consequence of the strategy of mystery composing is finished among the benefactor aspect with various sorts and execution of PCs.

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 $r.e \equiv 1 \bmod \varphi(n)$ and $1 < e < \varphi(n)$.
6. Compute d such as $d.e \equiv 1 \bmod \gamma(n)$ 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 :
$$c = ((m^e \bmod n)^e \bmod n)$$
After that Entity A will send c to entity B.

C. Decryption Process

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

Fig. 2. Key Generation Algorithm

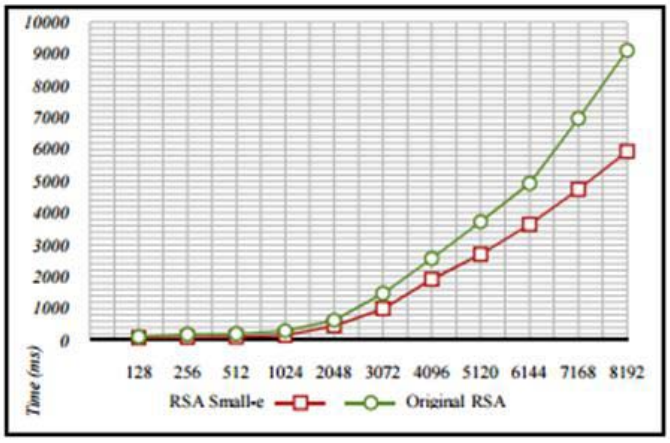

Fig. 3. Effects of changing key size

C. *Encryption and Decryption Time*

Cryptography Agent (CGA) was printed to figure data before putting away in cloud servers. This mystery composing made by HE-RSA calculation by exploitation twin mystery composing and maybe a couple of completely, entirely unexpected cryptography keys upheld RSA calculation which can upgrade the assurance in cloud servers. As was appeared in figure thus the character of RSA Small-e, mystery composing

time might be a smaller amount than cryptography time extended. The season of cryptography should be eighty 5 p.c over mystery writing in old and the same circumstance, yet among the arranged model, the key composition approach is finished in customer with a low execution as contrasted and the cloud-based application. Accordingly, the brilliance between mystery composing and cryptography time is debilitated to 45 PC a few.

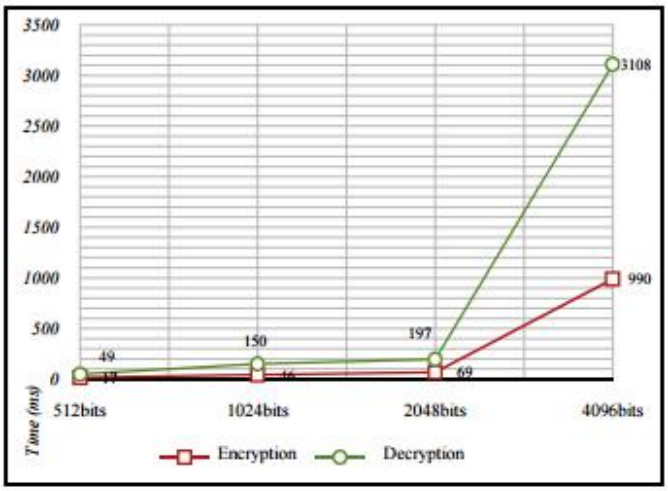

Fig. 4. Effects of changing key size on Encryption and Decryption

D. Total Execution Time

The procedure of client validation in the anticipated model was reproduced by four types of key sizes. Besides, this recreation was contrasted and the standard client validation strategy the resulting figure demonstrates this examination in points of interest:

VI. ANALYSIS AND EVALUATION OF MODEL

The following parameters are chosen for evaluation of the proposed model:

A. Scalability:

Cloud based structure turns out to be further climbable here subsequently of the educated model uses different apparatuses and systems. Dependency of the strategy for cloud ceased operations has been impressively lessened utilizing a customer based client .By this de-wrinkle, the strategy of validation turns out to be further climbable. In addition, utilization of

Partitioned verification programming ease-an administration of principle cloud servers will build the

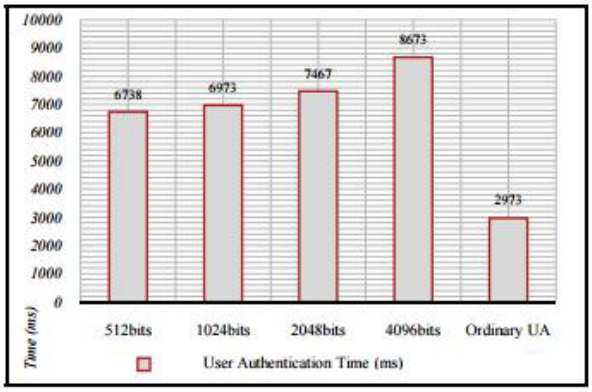

Fig. 5. Comparison the time of user authentication between the proposed model and ordinary user authentication

Flexibilities of overseeing validation at a comparable time. The use of discrete operators makes the mode assist reasonable.

B. Efficiency:

The intensity of the arranged model is extra by using intelligent and shabby correspondences between discrete specialists. Therefore, every operator ensures the personality of client independence, however, this can benefit from outside assistance by option specialist against suspicious verifications. Moreover, by expanding the part of clients inside the strategy for defensive and getting to their own data is that the option, highlight of arranging model that will build intensity and also the responsiveness in the distributed computing air.

C. Security:

Security of the asked demonstrate has been enhanced consider by misuse various apparatuses and systems all through authentication and moreover data assurance forms. By setting up two styles of coding all through confirmation and before putting away data in cloud servers improves the speed of trust inside the structure. Besides, the arranged model is unimaginable solid and oppose against various assaults as takes after:

1) *Man in the Middle Attack*: to protect the asked show from Man inside the Middle assault, encoded answers (R1 and R2) and shared verification amongst MDHA and end-client is required. For this reason client figures Kuser=R1Y mod G and E=Encrypt(R2,Kuser)and sends R2,E to MDHA. By this strategy, MDHA registers KMDHA=R2Xmod G and R3=Decrypt(E,KMDHA).These forms hinder the individual inside the Middle assault and by investigation R2and R3 the assault are known. In accordance with this examination, R2and R3are not same for MDHA thus of the keys amongst clients and aggressors square measure entirely unexpected.

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

2) *Brute Force Attack*: amid this attacker tries every single possible combo to figure the non-open key. Exploitation HE-RSA inside the arranged model makes this algorithmic pro-gram has indispensable oppose against animal compel assault by 1024 bits of type size, though, the underlying RSA might want 2048 example size to oppose against this assault [18].

3) *Timing Attack*: amid this assault, attacker decides non-open type of canny the time with abusing the fleeting request variety of the standard operation [19]. The learning is master tested by exploitation twin mystery writing in HE-RSA before putting away information to cloud and its not expected to increase information to stop this assault.

4) *Privacy of User Data*: The planned theme ne'er transmits the information of user in plain text type. The messages square measure transmitted over the general public channel. Thus, the time provides user privacy.

5) *Mutual authentication*: during this time, authentication is performed on each shopper in addition as server facet. This provided additional reliableness. Hence, mutual authentication is performed.

6) *Phishing attack*: Mutual authentication is performed dur-ing this theme between the user and also the server .Therefore, solely the real server will send correct user identification knowledge which is able to be eventually verified by the user. Hence, the theme is powerful against phishing attacks.

7) *Insider attack*: corporate executive attack: Insider attack is an extremely venturesome threat to any inter-networking system. Within the planned theme, the watchword isn't used overtly, instead, it's encrypted victimization Access code generation that is extremely tough to invert. Hence, the theme is powerful against corporate executive attack additionally.

VII. CONCLUSION

Considering the challenges and problems throughout user authentication and access management in the cloud and con-jointly considering the safety problems touching on cloud primarily based environments, associate degree economical and ascendible user authentication theme was projected during this paper. In the guided mode, changed devices and strategies were presented by exploitation the build of specialist. In this way ,to show the personality of client in customer viewpoint a customer based client confirmation operator was presented. Besides, a cloud-based programming as-an administration application for affirming the technique for confirmation for unregistered gadgets. Also, 2 isolate servers for putting away validation and cryptography assets from fundamental servers are needed to diminish the reliance of client verification and coding forms from the primary server. Cryptography specialist was conjointly acquainted with engrave assets before putting away all assets on cloud servers. By and large, the hypothetical investigation of the directed subject demonstrates that to accomplish and upgrade duty ,planning this client validation relate degrees get to administration model can encourage in accomplishing that and moreover it'll expand the speed of trust in distributed computing conditions as a rising and effective innovation in fluctuated businesses.

VIII REFERENCES

[1] A. Vandenberg, W. Han, and N. Xiong, Green cloud computing schemes based on networks: a survey, IET Communications, vol. 6, no. 18, pp. 3294-3300, December 2012.

[2] H. Tianfield, Security issues in cloud computing, in Proc. IEEE Inter-national Conference on Systems, Man, and Cybernetics (SMC), 2012, Seoul, South Korea, pp. 1082-1089

[3] H. Latifi, A. Hakemi, and N. Memari, A Reliable E-Service Framework based on Cloud Computing Concepts for SaaS Applications, in Proc. IEEE Conference on e-Learning, eManagement and e-Services (IC3e), 2013, pp. 100-104.

[4] O. Karimi, M. T. Alrashdan, and F. Fatemi Moghaddam, 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. 238241, 2013

[5] L. Lamport, Insecure communication with Password authentication, Comm. ACM 24(11), Nov 1981, 770-771

[6] L.H. Li and, M.S.Hwang, Using Smart Cards Provide New Remote User Authentication Scheme, IEEE Transactions on Consumer Electronics 46
(1)(2000) 28-30.

[7] M.K. Khan, Cryptanalysis and Security Enhancement of Two Password Authentication Schemes with Smart Cards, INMIC 2007 and Multitopic Conference, 2007. IEEE International.

[8] K. Lauter and S. Kamara, Financial Cryptography and Data Security, Cryptographic Cloud Storage, Lecture Notes in Computer Science, vol. 6054, pp 136-149, 2010.

[9] H. J. Wang, D. Molnar, R. A. Popa, , and L. Zhuang Enabling security in cloud storage SLAs with cloud-proof, in Proc. USENIX Annual Technical Conference,Microsoft Research, June 2011.

[10] M. Sain ,P. Kumar, A.J. Choudhury, , 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.

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

[12] M. T. Alrashdan,M. Hajivali, and A. Alothmani, Access Control Model for Cloud Servers on Apply an Agent.

[13] Based User Authentication, in Proc. IEEE International Conference on ICT Convergence, South Korea, Jeju Island October 2013, Pages: 807-812.

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

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

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

[17] O. Karimi, M. T. Alrashdan, and F. Fatemi Moghaddam, 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.

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

[19] Paul C. Kocher, Timing Attacks on Implementations of RSA,DSS Diffie Hellman, and Other Systems, in Proc. 16th Annual International Cryp-tology Conference on Advances in Cryptology (CRYPTO96), London, 1996, pp. 104-113.

[20] A .M. Haque and A. Alhasib, A Comparative Study of the Perfor-mance and Security Issues of RSA AND AES Cryptography, in Proc. 3rd Interna-tional Conference on Convergence and Hybrid Information Technology (ICCIT), Busan, 2008, pp. 505-510.