RESEARCH ARTICLE OPEN ACCESS

A Study of Pairing-Free Identity-Based Mutual Authenticated Protocol for Cloud Computing

Vinod Kumar*,Musheer Ahmad*,Adesh Kumari**,Pankaj Kumar***
**(Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi, India*
*** (Bhawan Mahavir College of education Sonepat, Haryana, India*
**** (Departments of Mathematics, Ramjas College, University of Delhi, New Delhi, India*

ABSTRACT
Many companies start to provide various kinds of cloud computing services for internet users at the same time these services also bring several security issues. Currently the greater part of cloud computing systems provides digital identity for users to get access to their services. Presently, most of the cloud computing system use asymmetric and conventional public key cryptography to give mutual authentication data security. Pairing-free identity based cryptography has some pull characteristics that give the impression to fit find the requirements of cloud computing. The proposed protocol accomplishes in three phases such as initialization phase, registration phase and mutual authentication and session key agreement phase. Detailed security analyses have been made to authenticate cloud server and user. Further, the paper has resistance to possible attacks in cloud computing.

Keywords **-** Anonymity, Cloud Computing, Smart Card, Elliptic Curve Cryptography, Mutual Authentication and Security

---

Date of Submission: 11 -07-2017 Date of acceptance: 31-07-2017

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large collection of systems are connected in private or public networks, to offer enthusiastically scalable infrastructure for data, application, and file storage. With the arrival of this technology, the cost of computation, relevance hosting, content storage and release is reduced significantly. Cloud computing is a practical approach to experience direct cost profits and it has prospective to convert a data center from a capital-intensive arrangement to a variable priced background. A user can access or control via the Cloud infrastructure lacking knowledge, expertise and speculation [1]. Advocates declare that cloud computing permits companies to stay away from up-front transportation costs (e.g., purchasing servers). Like as, it facilitates associations to focus on their foundation businesses as an alternative of spending time and money on computer communications. Promoters also declare that cloud computing tolerates enterprises to get their appliances up and running faster, with improved manageability and less maintenance, and enables in order technology teams to more speedily regulate possessions to congregate changeable and impulsive business stipulate. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model. The objective of cloud computing is to permit users to take benefit from all of these technologies, with no require for unfathomable information about or knowledge with every one of them. The cloud aspires to cut costs, and assists the users spotlight on their interior business in its place of being impeded by IT obstacles.[12] the major enabling skill for cloud computing is virtualization. Virtualization software splits a corporal computing apparatus into one or more "virtual" devices, every of which can be easily used and managed to execute computing tasks. With operating system–level virtualization fundamentally producing a scalable system of several independent computing devices, idle computing resources can be owed and used more resourcefully. Virtualization offers the quickness required to speed up IT procedures, and decreases cost by increasing transportation utilization. Autonomic computing automates the development throughout which the user cans stipulation resources on-demand. By minimizing user contribution, computerization speeds up the procedure, reduces employment costs and reduces the opportunity of human errors. On the other hand, there are various issues that require to be attended to accomplish stretchy and secure infrastructure. Zhang et al. [11] presented a brief study of the research challenges which are occurring in Cloud. Takabi et al. [8] argued the budding securities in it. One of the challenges is to control the data violating in cloud storage services. Since, user stores/access her/his data over the remote server, an adversary know how to get the

opportunity to makes that system defenseless for attack as an adversary can attain fully control over the public network attain safe and approved communication, a dominant mutual authentication and session key establishment protocol is necessary. [7]. Anonymity of user and server identity also enhances the security as an adversary is not able to relate previously gained information. Therefore, secure and anonymous mutual authentication mechanism is paramount requirement in cloud.

There are several security issues in cloud computing service environments, serviceability, traffic management, application security, access control, including virtualization, distributed big-data processing authentication, and cryptography, among others.[4]. In 1984 Shamir proposed the concept of ID-Based Cryptography (IBC) to remove the authentication, communication, and protection of public key certificates [2]. Hankerson et al [5], presented Background of Elliptic Curve Cryptography (ECC) and its techniques. In modern, many identity-based authentication protocols have been proposed for cloud [10, 3, 6]. In 2009, Yang et al [10] proposed an identity-based remote user authentication protocol for mobile users based on elliptic curve cryptography (ECC). Their scheme inherits the merits of both identity based cryptosystem and elliptic curve. Chen et al. [3] identified two security flaws, namely, insider attack and impersonation attack in Yang-Chang's scheme. To remove these security flaws, they presented an advanced password based authentication scheme. The authors claimed that their protocol is secured to provide mutual authentication and is appropriate for Cloud Computing environment. However, in 2012, Wang et al. [9] showed that Chen et al. scheme is not secure and is susceptible to offline password guessing attack and key compromise impersonation attack and also suffers from clock synchronization problem. Kang and Zhang [6] protocol, which requires the computation of bilinear pairing on super singular elliptic curve (EC) group with large element size somewhere the computation cost of the pairing is approximately three or more times higher than that of EC point multiplication. Mishra et al [7] have proposed a pairing-free identity based authentication framework for cloud computing and also found that their scheme suffers some serious security flaws. Chen et al [3] presented an advanced ECC dynamic ID-based remote mutual authentication scheme for cloud computing, I found that their scheme suffer in hash functions, those are used finding session keys and message authentication codes (MAC).

In this paper, we presented a study of pairing-free identity-based mutual authenticated protocol for cloud computing. The remaining paper is structured in the following way: 2. Preliminaries, 3.The proposed protocol, 4.Security Analysis, 5. Performance analysis and 6.Conclusion.

II. MATHEMATICAL PRELIMINARIES

1. Background of Elliptic Curve Cryptography

Let q is the large prime and, E denote an elliptic curve over a prime finite field F_q, defined by an equation $y^2 = x^3 + ax + b \mod q$ with $a, b \in_R F_q$ and $4a^3 + 27b^2 \mod q \neq 0$. The additive elliptic curve group defined as $G = \{(x, y): x, y \in_R F_q ; (x, y) \in_R E\} \cup \{\Theta\}$, where the point Θ is known as point at infinity which act as the identity element in P. The point addition in elliptic curve as: If $P = (x_P, y_P) \in_R G$ and $Q = (x_Q, y_Q) \in_R G$, Where $P \neq Q$ then $P + Q = (x_i, y_i)$, where $x_i = \mu^2 - x_P - x_Q \mod q$, $y_i = (\mu(x_P - x_Q) - y_P) \mod q$ and $\mu = (y_Q - y_P)/(x_Q - x_P)$. The scalar multiplication on the group G is defined like $tP = P + P + P \ldots \ldots + P(t\ times)$. The more details of elliptic curve group are given in [5].

2. Computational Problem

- **Elliptic Curve Discrete Logarithms Problem (ECDLP):** For given $P, Q \in_R G$ find $k \in_R Z_q^*$ such that $P = kQ$, which is hard.
- **Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP):** For $a, b \in_R Z_q^*$ and the g is the generator of G, given (g, ag, bg), then compute abg is hard to the group G.

III. THE PROPOSED PROTOCOL

In this session, the paper an improved pairing-free identity-based mutual authenticated Protocol. This protocol consists of the following three phases: Initialization phase, User registration phase and Mutual authentication and session key agreement.

1. Initialization phase

. Assume that server S play the role of private key generator (PKG) which takes a security parameter l, returns security parameter. For given l, S takes following steps

- Choose an arbitrary generator $g \in_R G$.
- Select a master key $p \in_R Z_q^*$ and public key $P_S = pg$.
- Choose collision free one way hash functions: $H_1: \{0,1\}^* \times Z_q^* \rightarrow Z_q^*$;
  $H_2: G \times G \times G \times G \rightarrow Z_q^*$;
  $H_3: \{0,1\}^* \rightarrow Z_q^*$;
  $H_4: \{0,1\}^* \times \{0,1\}^l \rightarrow Z_q^*$.

Publish systems parameters $< F_q, E, G, l, g, P_S, H_1, H_2, H_3, H_4 >$.

2. User registration phase

- User U submits her/his identities ID_U and password PW_U to S. Then, generate a random number $u \in_R Z_q^*$. Computes $PWU = H(PW_U \oplus u)$ and sends $< ID_U, PWU >$ to S.
- S Computes, user authenticated key $KID_U = P_S H_3(ID_U), B_S = H(ID_U \oplus PWU)$ and generates random number $s \in_R Z_q^*$. S Store smart card $< B_S, KID_S, H_1, H_2, H_3, H_4, s >$, where s is secret key shared to user.
- Upon receiving the smart card, U store random number in u in smart card. Hence smart card $< B_S, KID_U, H_1, H_2, H_3, H_4, s, u >$.
- User enters his/her ID_U and PW_U to verify whether $B_S = H(ID_U \oplus H(PW_U \oplus u))$. If it is hold U accepts the smart card.

3. Mutual authentication and session key agreement

Assume that user U asks a service from cloud server S. User U and server S mutually authenticate each other and establish a session key as:

Step 1. U sends his/her identity ID_U and password PW_U to login and perform as:

- ❖ Computes $B_U = H(ID_U \oplus PWU)$. Checks whether $B_U =? B_S$. If it is holds, then chooses a random number $R_U = (x_U, y_U) \in_R G$ and computes $U_1 = H_3(T_1)$, $M_U = R_U + U_1 KID_U$ at timestamp T_1 and anonymous identities $AID_U = ID_U \oplus H_4(ID_U || T_1)$.
- ❖ U Sends $< T_1, AID_U, R_U, M_U >$ to S. Where T_1 is the current date and time of user U.

Step 2. On getting the message, S computes $T_2 - T_1 \leq \Delta T$, where T_2 the message getting time of S and ΔT is the suitable time delay in message communication. If condition is hold, then S computes $KID_S = P_S H_3(ID_S)$. Where ID_S is the identity of sever S.

- ❖ S Generates random number $R_S = (x_S, y_S) \in_R G$, computes $S_1 = H_3(T_3)$, $M_S = R_S + S_1 KID_S$, session key $sk_S = H_2(M_S || M_U || R_S || R_U)$ and message authentication code $MAC_S = (sk_S + x_S)g$ at timestamp T_3.
- ❖ S Sends message $< T_3, M_S, R_S, MAC_S >$ to U. Where T_3 time and date sending message to U.

Step 3. On getting the message, U computes $T_4 - T_3 \leq \Delta T$ where T_4 the message receiving date and ΔT is the suitable time delay in message communication. If condition is hold, then U computes session key $sk_U = H_2(M_U || M_S || R_U || R_S)$ and message authentication code $MAC_U = (sk_U + x_U)g$; U Check the condition $MAC_U =? MAC_S$. If the condition holds S is authenticated by U with session key $sk = sk_U = sk_S$.

Finally, session establishes user can store/access his/her data securely over the public channel.

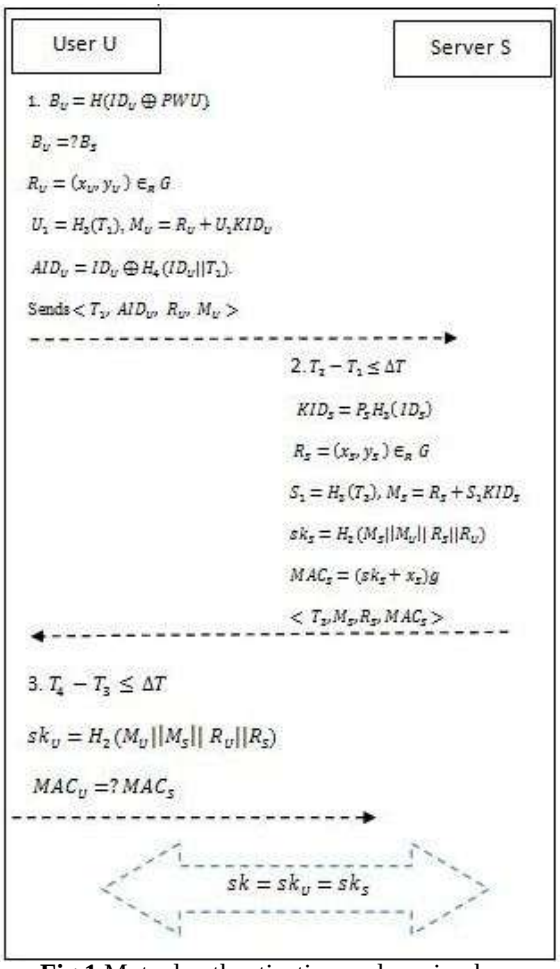

Fig.1 Mutual authentication and session key agreement

IV. SECURITY ANALYSIS

In this section, the proposed protocol secure against following security attacks:

- ❖ **Identity Management:** The server stores all the registered identities ID_U of users U in the database and check availability of unique identities in each new registration.
- ❖ **Anonymity:** In Mutual authentication and session key agreement, user sends anonymous identity $AID_U = ID_U \oplus H_4(ID_U || T_1)$ to cloud server instead of real identity ID_U. The identity ID_U is XOR with the hashed value of ID_U and T_1. Where assumed that hash function is secure in cryptosystem.
- ❖ **User Privacy:** The proposed scheme never transmits user private data in plaintext form. The messages $< T_1, AID_U, R_U, M_U, K_U >$ and $< T_3, M_S, R_S, MAC_S >$ are transmitted over the public channel. Evidently, these messages cannot be interpret easily to get identity,

password etc. Hence, the protocol provides user privacy.

- **Replay Attack:** Replay Attack is most common attack in authentication progression. On the other hand, the common countermeasures are time-stamp and random number mechanism. This protocol, adopt the counter-measure and time-stamp. The messages, Mutual authentication phase U → S and S → U are with time-stamps. Hence this protocol is strong against Replay attack.
- **Mutual Authentication:** Mutual authentication is a significant attribute for a verification service opposing to server spoofing attack. The proposed protocol provides a mutual authentication for the user U and server S by ECC-based private and public key exchange.
- **No Key Control:** In this protocol, user U and server S have an input into the session key neither accomplice can strength the full session key to be a preselected value. The session key $sk = H_2(M_U||M_S||R_U||R_S))$ depends on $M_U = R_U + U_1 KID_U$ and $M_S = R_S + S_1 KID_S$. So M_U or M_S depends on random number and hash function, therefore, any single user cannot manage the result of the session keys or impose others.
- **Man in the Middle Attack:** User and server authenticate each other without eloquent. An adversary or malicious user can try man in the middle attack by sending the forge memorandum. However, to authenticate each other user and server exchange message authentication code (MAC). To compute MAC, knowledge of session keys sk is required, although, session key sk is assumed secret and cannot be accomplished with publicly known values.
- **Key off-set Attack:** In the protocol, user U and server S authenticated each other and established session key $sk = H_2(M_U||M_S||R_U||R_S)$.User message authentication code $MAC_U = (sk_U + x_U)g$ and server message authentication code $MAC_S = (sk_S + x_S)g$. If $MAC_U \neq MAC_S$, user U rejects the session key agreement and sends an authentication-failed message to S. Therefore key off-set attack is not possible in this protocol.
- **Phishing Attack:** Mutual authentication between the user and the server is performed in this protocol. Only the genuine server can send proper user identification data, which will be verified by the user. Hence, the protocol is strong against phishing attack.
- **Session Key Agreement:** A session key $sk = H_2(M_U||M_S||R_U||R_S)$ is established between the user and the server after authentication process. This key is different for different users. Therefore adversary cannot access the session key of particular user.
- **Impersonation Attack:** The proposed protocol never transmits user's identity ID_U and password PWU unswervingly via the public channel. In its place, ID_U and PWU are hashed and performed several business over it. Therefore the proposed protocol is strong against impersonation attack.
- **Perfect forward Secrecy:** An adversary cannot compute session key because to compute session key $sk = H_2(M_U||M_S||R_U||R_S)$.Where to computes KID_S or KID_U is equivalent to ECCDHP in ECC.
- **PKG forward Secrecy:** An adversary cannot even compute the user or server message authentication code $MAC_U = (sk_U + x_U)g$ or $MAC_S = (sk_S + x_S)g$. To computes sk_U or sk_S is equivalent ECCDHP in ECC and computes MAC_U or MAC_S is equivalent ECDLP in ECC.

V. PERFORMANCE ANALYSIS

In this session, the paper discussed mutual authentication with key agreement phase which is the main computation cost of an authentication mechanism. This protocol is more secured than [3] and [7].

Computation cost	[3]	[7]	Proposed
Mutual authentication and session key agreement	13H + 2EC+ 6PM+ 4PA	6H+ 2EC + 12PM+ 2PA	7H+ 2EC+ 5PM+ 2PA

Where **H:** Hash function; **EC:** Elliptic curve polynomial operations; **PM:** Elliptic curve point multiplication operations; **PA:** Elliptic curve point addition operations.

VI. CONCLUSION

The paper has presented pairing-free identity-based mutual authentication protocol which is highly secured mutual authenticated in cloud environment. Here, user and server mutually authenticated to each other and established session key over public networks. Further, the paper shows the security analysis of this protocol against several security attacks in cloud atmosphere. Lastly, it showed performance of this protocol which is more efficient compare with Mishra et al [7] and Chen et al[3].

REFERENCES

[1]. Armbrust, et al.: A View of Cloud Computing. Communications of the ACM, 53(4), 2010, 50–58.
[2]. X. Cao, W. Kou and X. Du, A Pairing-free Identity-based Authenticated Key Agreement Protocol with Minimal Message Exchanges, Information Sciences, 180, 2010, 2895−2903,.
[3]. T. H. Chen, H. Yeh and W. Shih, An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing, 2011 Fifth FTRA International Conference on Multimedia and Ubiquitous Engineering, IEEE Computer Society, 2011,155-159.
[4]. C. Choi, J. Choi and P. Kim, Ontology-based Access Control Model for Security Policy Reasoning in Cloud Computing, Springer Science Business Media New York 2013, DOI 10.1007/s11227-013-0980-1.
[5]. D. Hankerson, A. J. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.
[6]. L. Kang and X. Zhang, Identity-Based Authentication in Cloud Storage Sharing, International Conference on Multimedia Information Network and Security (MINES), IEEE Computer Society, 2010, 851–855.
[7]. D. Mishra, V. Kumar and S. Mukhopadhyay, A Pairing-Free Identity Based Authentication Framework for Cloud Computing, LNCS 7873,Springer-Verlag Berlin Heidelberg,2013, 721–727.
[8]. H. Takabi, J. B. D. Joshi and G. J. Ahn, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, 8(6), 2010 24–31.
[9]. D. Wang,Y. Mei, Y.,C. G. Ma and Z. S. Cui, Comments on an advanced dynamic ID-based authentication scheme for cloud computing, In: Wang, F.L., Lei, J., Gong, Z., Luo, X. (eds.) WISM 2012", LNCS, Springer, Heidelberg, 7529, 2012, 246-253.
[10]. J.H., Yang, and C.C. Chang, An ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on Elliptic Curve Cryptosystem, Computers & Security, 28(3), 2009, 38–143.
[11]. Q. Zhang, L. Cheng and R. Boutaba, Cloud Computing: State-of-the-art and Research Challenges, Journal of Internet Services and Applications, 1(1), 2010, 7–18.
[12]. M.Hamdaqa, L.Tahvildari, Cloud Computing Uncovered: A Research Landscape, Advances in Computers, 86, 2012, 41-85.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Vinod Kumar. "A Study of Pairing-Free Identity-Based Mutual Authenticated Protocol for Cloud Computing." International Journal of Engineering Research and Applications (IJERA) 7.7 (2017): 10-14.