An Identity-Based Secure Authenticated Framework by Using ECC in Cloud Computing

Nasheem Khan[1], **Vinod Kumar**[2], **Adesh Kumari**[3]

[1] University of Delhi, Department of Mathematics, Kamala Nehru College, August Kranti Marg, New Delhi-110049, India

[2,3]University of Delhi, Department of Mathematics, Deshbandhu College, Kalkaji, New Delhi-110039, India

Abstract: ***Cloud Computing with Elliptic Curve Cryptography (ECC) is an entirely novel area and has inconceivable scope of research. It is a talented saleable infrastructure archetype that promises to exterminate require for maintaining exclusive computing amenities by companies and institutes comparable. It has obsessed insubstantial, technical, economic, and client experience characteristics. All through the use of virtualization and resource time allocation, clouds provide with a testing position of physical resources a gargantuan client base with dissimilar requirements. However, a user uses public network for the duration of right of entry of cloud services at the same time an adversary knows how to get full control over the public network. Therefore, a user ought to advocate a mechanism in which user and server can authenticate each other and generate a safe session. In this projected protocol, user and server established a session key and can communicate securely through the public network. This recently protocol decreases the cost of computation deeply and compared with previous existing protocol. Detailed network security investigations have been made to authenticate the proficiency of the protocol. Additional, this protocol has the argument to likely attacks in cloud computing.***

Keywords: Cloud Computing, Elliptic Curve Cryptography, Pairing-free Identity based Cryptosystem, Authentication, Private Key Generator and Security.

1. Introduction

Cloud computing is the speedy rising Internet based technology that tolerates computer assets to be collective on an on-demand foundation. In cloud computing user do not sentient as regards, where data is accumulated and how their data is being processed. They simply admittance data development and lastly store them in the cloud. Also, they can access data at anytime, anyplace if they are having Internet connection. This technology is greatly scalable, distributed in nature and flexible. In cloud computing computational resources are provided to the end-user as a service [10].It is a model for enabling suitable on-demand admittance to servers, storage, functions, networks and services which can be quickly provisioned and unrestricted with smallest organization exertion or service provider communication. It is an imaginative client-server construction that accomplishes the user's hardware necessities and diminishes generally user side requirements and complicatedness. Yet, there is require for a uniform definition of cloud computing. the paper adopts, definition of NIST characterization in cloud computing "a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [8]. Cloud Computing Technology mainly partitioned into five types of public cloud computing such as: Software as a Service (SAAS), Platform as a Service (PAAS), Data Storage as Services (DSAAS), Network as a Service (NAAS) and Infrastructure as a Service (IAAS). The more information of the concepts, characteristics and architecture in cloud computing [6, 5].

Currently, cloud computing is newly developed technology, there are many issues such as data portability, ownership, conversion, multiplatform support, data backup, reliability and many more. Among all these issues security is the most important issue. Security issues involve virtualization security, distributed computing security, access control, application security, identity management, authentication [1]. In 1984 Shamir proposed the concept of ID-Based Cryptography (IBC) to remove the authentication, announcement, and protection of public key certificates. In IBC client's unique identity, like as rather than a random number, e-mail address, as the client's unrestricted key, and the client's equivalent private key is generated based on the client's unrestricted key by the system's trusted organization. The organization's trusted authority is incomparable and is the represents of the IBC. It is called Private Key Generator (PKG) or Key Generate Centre (KGC) [2]. In current years, several identity-based authentication protocols have been proposed for cloud [4, 7, 13]. Yang and Chang [13] proposed an identity-based remote user authentication protocol for mobile users based on elliptic curve cryptography (ECC). This protocol succeeds to the qualities of both identity based elliptic curve and cryptosystem. To remove these security flaws, Chen et al. Presented an advanced password based authentication protocol, which is secured to provide mutual authentication and is appropriate for Cloud Computing atmosphere [4]. In 2012, Wang et al. [12] showed that Chen et al. protocol is not protected and weak to offline password guessing attack and key compromise impersonation attack and also undergo from clock synchronization problem. Kang and Zhang [7] proposed short key size identity based authentication protocol, which involves the computation of bilinear pairing on super singular elliptic curve group with large element size where the computation cost of the pairing is approximately three times more than that of elliptic curve point multiplication. In 2013 Mishra et. al [9] presented a pairing-free identity based authentication framework for cloud computing which show identity based authentication and security in cloud environment using different attacks. In addition to authentication it also provides session key between the client and server and mutual authentication [3, 14].

This paper presents An Identity-Based Secure Authenticated Framework by Using ECC in Cloud Computing. The rest of the paper is organized as follows. 2. Preliminaries, 3.The proposed protocol, 4.Security Analysis, 5.Performance analysis and 6.Conclusion.

2. Preliminaries

2.1 Notations

Symbols	**Meaning**
P	A large prime number
$\mathbb{F}_P$	Prime finite field
$\mathbb{E}$	An elliptic curve over a prime finite field
$\mathbb{G}$	Additive elliptic curve cyclic group
$\mathcal{G}$	Generator of group $\mathbb{G}$
$\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$	Cryptographic secure hash functions
m	Master key of PKG
$\mathrm{P_{pub}}$	The public key of PKG
ID_i	The entity$i$'s identity
PK_i	Private Key of entity i
sk	Secure session key

2.2 Computational Problem Elliptic Curve Cryptography

Elliptic Discrete Logarithms Problem (EDLP): For given $\mathrm{A, B} \in_{\mathrm{R}} \mathbb{G}$ find $\mathrm{k} \in_{\mathrm{R}} \mathrm{Z_P^*}$ such that $\mathrm{A = kB}$, which is hard.

Elliptic Computational Diffie-Hellman Problem (ECDHP): For $x, y \in_{\mathrm{R}} \mathrm{Z_P^*}$ and the $\mathcal{G}$ is the generator of $\mathbb{G}$, given$(\mathcal{G}, \mathrm{x}\mathcal{G}, \mathrm{y}\mathcal{G})$, then compute $\mathrm{xy}\mathcal{G}$ is hard to the group $\mathbb{G}$.

3. The Proposed Protocol

The protocol is composing of major three algorithms:

3.1 Set Up

Private Key Generator (PKG) takes a security parameter k, returns security parameter and master key m for given k, PKG takes following steps:

Choose an arbitrary generator $\mathcal{G} \in \mathbb{G}$.

Select a master key $\mathrm{m} \in \mathrm{Z_P^*}$ and public key $\mathrm{P_{pub}} = \mathrm{m}\mathcal{G}$.

Choose collision free one way hash functions

$\mathcal{H}_1 : \{0,1\}^* \times \mathbb{G} \to Z_P^*$.

$\mathcal{H}_2 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^k \times \mathbb{G} \times \mathbb{G} \to \{0,1\}^k$.

$\mathcal{H}_3 : \mathbb{G} \times \{0,1\}^k \to Z_P^*$.

Publish systems parameters $< \mathbb{F}_P, \mathbb{E}, \mathbb{G}, k, \mathcal{G}, P, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 >$ and m keep secret.

3.2 Extraction

Entity i submits her/his public identities ID_i to PKG. Then PKG verifies the proof of identity. If verification succeeds, generates the partial private key as:

- Generate a random number $x_i \in Z_P^*$.
- Compute $I_i = x_i\mathcal{G}$ and $h_i = \mathcal{H}_1(ID_i||I_i)$.
- PKG generate the partial private key as$J_i = x_i + mh_i$. Then PKG distributes user partial private key via a secure channel.

On receiving partial private key entity i checks the condition$J_i\mathcal{G} = I_i + \mathcal{H}_1(ID_i||I_i)\mathrm{P_{pub}}$. Then entity i sets public key $PK_i = J_i\mathcal{G}$.

3.3 Authentication and Key Agreement

User U and server S mutually authenticate each other and establish a session key as:

- U Generate a random number $r_U \in_R Z_P^*$, an opaque string sid as a session identity and computes $K_U = r_U PK_U$ and sends $< ID_U, sid, K_U, T_1 >$ to S. Where T_1 is the current date and time of U.
- On receiving message, S computes $T_2 - T_1$, checks $T_2 - T_1 \le \Delta T$. Where T_2 message receiving time of S and ΔT is the valid time delay in message transmission. If condition is hold then, S generate a random number $r_S \in_R Z_P^*$, computes $K_S = r_S PK_S$, mutual authenticated code $MAC_S = \mathcal{H}_2(ID_S||ID_U||sid||K_U||K_S)$ and sends $< ID_S, MAC_S, K_S, T_3 >$ to U. Where T_3 is the current date and time of S.
- On receiving message, U computes $T_4 - T_3$, checks $T_4 - T_3 \le \Delta T$. Where T_4 message receiving time of user U and ΔT is the valid time delay in message transmission. If condition is hold then, U generates random number $r_{U1} \in_R Z_P^*$, computes mutual authenticated code $MAC_U = \mathcal{H}_2\big(ID_U\big|\big|ID_S\big|\big|sid\big|\big|K_S\big|\big|K_U\big)$, session key $sk_U = r_{U1} + \mathcal{H}_3(r_U K_S||MAC_U)$, and sends $< ID_U, MAC_U, T_5 >$ to U. Where T_3 is the current date and time of U.
- On receiving message, S computes $T_6 - T_5$, checks $T_6 - T_5 \le \Delta T$. Where T_6 message receiving time of S and ΔT is the valid time delay in message transmission. If condition is hold then, also checks $MAC_S =? MAC_U$, if verified then, S generates random number $r_{S1} \in_R Z_P^*$, computes session key $sk_S = r_{S1} + \mathcal{H}_3(r_U K_S||MAC_S)$.

From the explanation of this protocol, S and U agreed session key can be computed as: $sk = sk_S = sk_U$. And, once the session establishes user can store/access his/her data strongly via the public channel.

4. Security Analysis

In this section, we have to discuss security analysis of 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.
- **Perfect forward Secrecy:** An adversary cannot compute session key because to compute session key $sk = r_{S1} + \mathcal{H}_3(r_U K_S||MAC_S) = r_{U1} + \mathcal{H}3rUKS||MACU$, Where to computes KS or KU is equivalent to ECDHP in ECC.

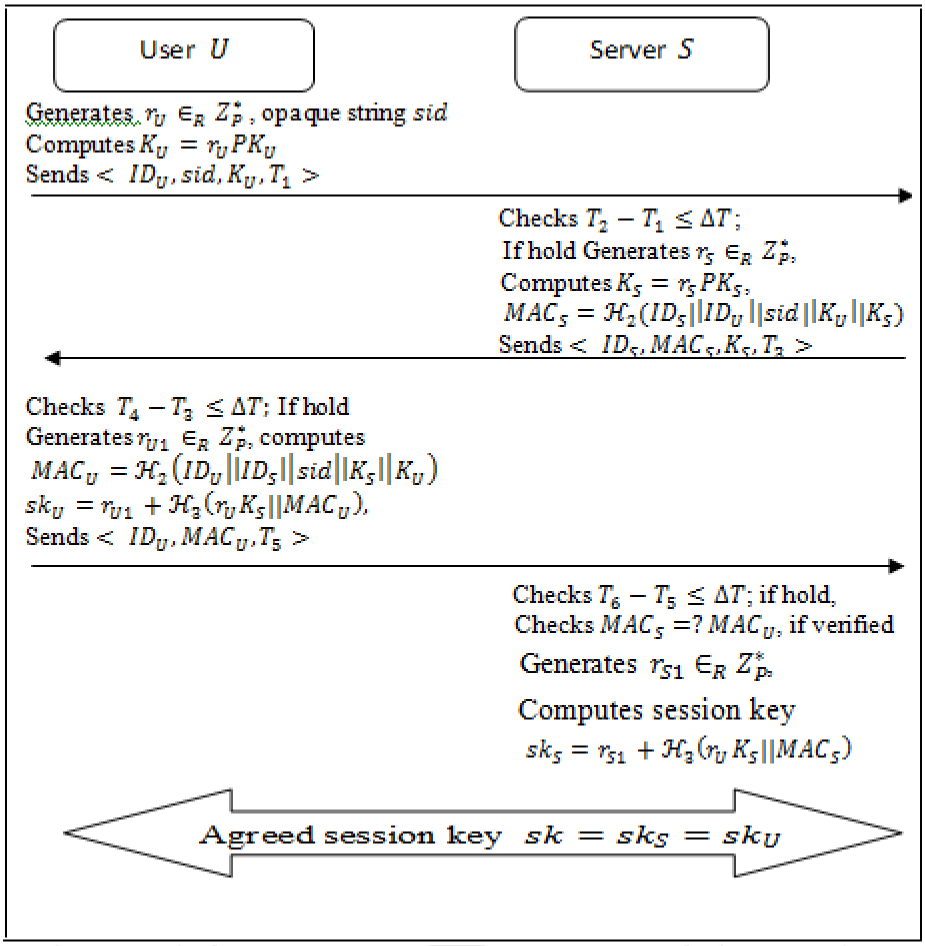
User U
Server S
Generates $r_U \in_R Z_P^*$, opaque string sid
Computes $K_U = r_U PK_U$
Sends $< ID_U, sid, K_U, T_1 >$
Checks $T_2 - T_1 \leq \Delta T$;
If hold Generates $r_S \in_R Z_P^*$,
Computes $K_S = r_S PK_S$,
$MAC_S = \mathcal{H}_2(ID_S||ID_U||sid||K_U||K_S)$
Sends $< ID_S, MAC_S, K_S, T_3 >$
Checks $T_4 - T_3 \leq \Delta T$; If hold
Generates $r_{U1} \in_R Z_P^*$, computes
$MAC_U = \mathcal{H}_2(ID_U||ID_S||sid||K_S||K_U)$
$sk_U = r_{U1} + \mathcal{H}_3(r_U K_S||MAC_U)$,
Sends $< ID_U, MAC_U, T_5 >$
Checks $T_6 - T_5 \leq \Delta T$; if hold,
Checks $MAC_S =? MAC_U$, if verified
Generates $r_{S1} \in_R Z_P^*$
Computes session key
$sk_S = r_{S1} + \mathcal{H}_3(r_U K_S||MAC_S)$
Agreed session key $sk = sk_S = sk_U$

Fig: Authentication and Key Agreement

- **Session Key Agreement:** A session key sk is recognized between the U and S then, authentication development. The session key is different for different users. Hence adversary cannot access the session key of particular user.
- **Mutual Authentication:** Mutual authentication is a significant attribute for a verification service opposing to server parodying attack. This protocol provides a mutual authentication between user and server by ECC-based private and public key exchange.
- **User Privacy:** The proposed Protocol never transmits user private data in message form. The messages $< ID_U, sid, K_U, T_1 >$ and $< ID_U, MAC_U, T_5 >$ are transmitted via the open channel. Manifestly, these messages cannot be interpret easily to get identity, password etc. Hence, the proposed protocol provides user privacy.
- **Replay Attack:** Replay Attack is most general attack in authentication development. On the other hand, the common countermeasures are time-stamp and random number instrument. The proposed protocol, accept the counter-measure and time-sstamp. The authentication phase $U \rightarrow S$ and $S \rightarrow U$ are with time-stamps. Hence the proposed protocol is strong against Replay Attack.
- **Man in the Middle Attack:** User and server authenticate each other without persuasive. An adversary or malicious user can try man in middle attack by sending the forge message..However, to authenticate each other user and server exchange message authentication code (MAC). To compute MAC, knowledge of hashed value required, although, hashed is assumed secret and cannot be finished with publicly known values.
- **Phishing Attack:** Mutual authentication between the user and the server is performed in the proposed protocol. Only the legitimate server can launch appropriate user classification data, which will be verified by the user. Hence, the protocol is strong against phishing attack.
- **No Key Control:** In the proposed protocol, user U and server S have an input into the session key neither accomplice can power the full session key to be a preselected value. The session key $sk = r_{S1} +$ $\mathcal{H}3rUKS||MACS=rU1+\mathcal{H}3rUKS||MACU,$ depends on $K_U = r_U PK_U$ and $K_S = r_S PK_S$ those are computes like as ECDHP in ECC. Moreover, sk depends on random number and hash function, therefore, any single user cannot handle the result of the session keys.
- **Session Key Agreement:** A session key sk is recognized between the U and S then, authentication development. The session key is different for different users. Hence adversary cannot access the session key of particular user.
- **Perfect forward Secrecy:** An adversary cannot compute session key because to compute session key $sk = r_{S1} + \mathcal{H}_3(r_U K_S||MAC_S) = r_{U1} +$ $\mathcal{H}3rUKS||MACU,$ Where to computes KS or KU is equivalent to ECDHP in ECC.

5. Performance Analysis

In this session, the paper discussed Authentication and Key Agreement phase which is the main computation cost of an authentication mechanism. This protocol is more secured than [4] and [9].

Computation cost	[4]	[9]	Proposed
Authentication and Key Agreement	13HA+2E+6EPM+4EPA	6HA+2E+12EPM+2EPA	4HA+2E+2EPM+2EPA

Where **HA:** Hash function; **E:** Elliptic curve polynomial operations; **EPM:** Elliptic curve point multiplication operations; **EPA:** Elliptic curve point addition operations.

6. Conclusion

Authentication between User and Cloud Sever is critical certification in data security which is also necessary in Cloud Computing. The paper shows the security analysis of this protocol. By the analysis of performance, this protocol is more efficient compare than Chen at al[4] and Mishra et al[9] in cloud environments. In addition to, the protocol is permitted by a budding cryptographic technique from the pairing-free and its security can be assured by EDLP and ECDHP.

References

[1] M. S. Blumenthal. “Hide and Seek in the Cloud”, Security & Privacy IEEE, PP. 57-58, 2010.
[2] X. Cao, W. Kou, and X. Du, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges”. Information Sciences, pp. 2895-2903, 180, 2010.
[3] O. Cheikhrouhou, A. Koubaa, M. Boujelben and M. Abid “ A lightweight user authentication scheme for Wireless Sensor networks”. IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2010.
[4] 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, pp.155-159.2011.
[5] H. A. Dinesh and V. K. Agrawal “Multi-level authentication technique for accessing cloud computing”, International conference on computing, communication and application (ICCA). IEEE Computer Society. pp. 1-4. 2012.
[6] X. Jing and Z. Jian-jun “ A brief survey on the security model of cloud computing”. Ninth international symposium on distributed computing and applications to business, Engineering and Science. IEEE Computer Society. pp. 475-478, 2010.
[7] L. Kang and X. Zhang “Identity-based authentication in cloud storage sharing”. In: International conference on multimedia information network and security (MINES). IEEE Computer Society. pp. 851-855, 2010.
[8] P. Mell, and T. Grance “ The NIST definition of cloud computing”53(6), 2009.
[9] D. Mishra, V. Kumar, and S. Mukhopadhyay “ A pairing-free identity based authentication framework for cloud computing”, NSS 2013, LNCS 7873, Springer-Verlag Berlin Heidelberg, pp. 721-727,2013.
[10] M.A.. Morsy, J. Grundy, and I. Muller “ An analysis of the cloud computing security problem”. In proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.
[11] H. Takbi,, J.B.D. Joshi, and G.J. Ahn,”Security and privacy challenges in cloud computing environments”. IEEE Security & Privacy pp. 24-31, 8(6), 2010.
[12] Wang et al, “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-7529, Springer Heidelberg, pp. 246-253, 2012.
[13] 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, pp. 138-143, 28(3), 2009..
[14] R. Yasmin, E. Ritter. And G. Wang. “ An authentication framework for wireless sensor networks using identity-based signatures”.10th IEEE International Conference on Computer and Information Technology, 2010.

Author Profile

Nasheem Khan received the B.Sc. and M.Sc. degree in Mathematics from Chaudhry Charan Singh University, Meerut,Uttar Pradesh, India,in 2006 and 2008.

Vinod Kumar received the M.Tech. in Computer Science and data Processing from Institute of Technology Kharagpur, Bengal, India in 2013. Also, received in M.Phil degree in Mathematics from Chaudhry University, Meerut,Uttar Pradesh, India in 2011.

Adesh Kumari received the Mathematics in 2009 from University, Rohtak, Haryana, India.