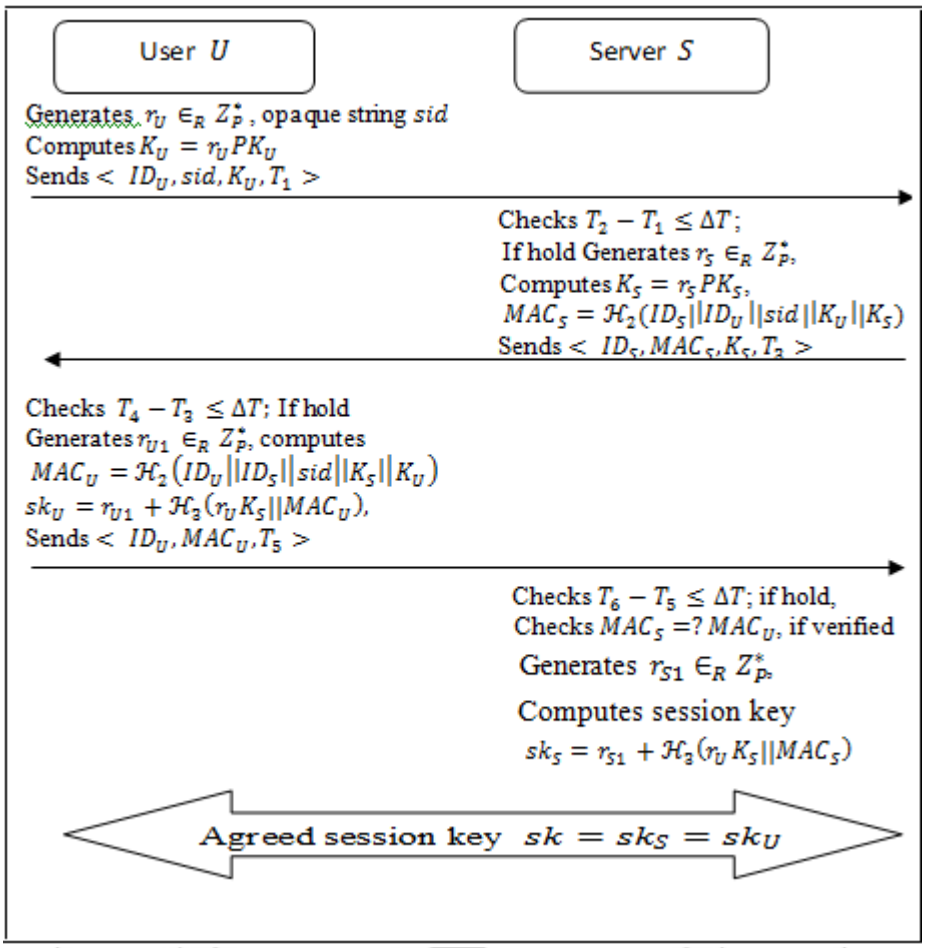

Fig: Authentication and Key Agreement

- **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].

Licensed Under Creative Commons Attribution CC BY

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.

Licensed Under Creative Commons Attribution CC BY