Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

An Efficient Secure and Privacy Preserving User Authentication Scheme for Mobile Cloud Computing Environment

K. Sandhya, S. Devika

[1]Assistant Prof, Dept. of CSE, Malla Reddy Institute of Technology & Science, Hyderabad.
[2]Assistant Prof, Dept. of CSE, Marri Laxman Reddy Institute of Technology, Hyderabad.

Abstract :- *As mobileusers for the most part get to various sorts of versatile distributed computing administrations from an assortment of specialist organizations, it is to a great degree dreary for users to enroll distinctive user accounts on each specialist organization and keep up relating private keys or passwords for validation use. In this paper, I propose an encryption technique call Attribute encryption strategy. Cloud computing is a progressive registering worldview, which empowers adaptable, on-request, and minimal effort utilization of required assets, however the information is outsourced or put away to some cloud servers, and different protection concerns rise up out of it. This paper concentrates on information protection, anonymity, access control. Quality based encryption system appended characteristics alongside the information and just attributes are scrambled the information is kept as it may be. Quality based encryption method expanded the security, execution and diminishes the season of proposed framework.*

Keywords *Authentication scheme, Attribute Based Encryption, Anonymity, mobile cloud computing services.*

1. Introduction

Combination of cloud computing, mobile computing andwireless networks is called as Mobile Cloud Computing (MCC) to bring rich computational assets for mobileusers, organize administrators, and in addition cloud computing suppliers. The objective behind the utilization of MCC is to empower execution of rich mobile applications on a plenty of cell phones, with a rich user encounter. The effect of versatile cloud computing is imperative research field in mobile situated world, giving new supplements, utilization, and conveyance models for IT administrations. MCC gives the better business public doors for mobile system administrators and additionally cloud suppliers. All the more thoroughly, MCC can be characterized as "a rich mobile processing innovation that use loosened flexible assets of changed mists and system advances toward unlimited usefulness, stockpiling, and portability to serve a huge number of cell phones anyplace, whenever through the channel of Ethernet or Internet paying little heed to heterogeneous conditions and stages in view of the compensation as-you-utilize rule. In any case, there are three worries to be settled alongside the verification plot. As a matter of first importance, in this plan figuring effectiveness is genuinely considered, since cell phones have just generally restricted processing capacity in correlation with smart phones. Second, adequate security quality ought to be bolstered; since all messages are transmitted by means of a shaky WLAN or media transmission arranges, a foe can undoubtedly get, intrude, or change transmitting messages before they achieve the coveted beneficiary. What's more, security assurance on user accounts is a rising issue as personality disguise and character following have turned out to be regular assaults in remote versatile conditions. As versatile users for the most part get to Traditional single sign-on (SSO) plans, for example, Passport and PublicID are one conceivable answer for key administration issue. In such frameworks, users can get to different mobile distributed computing administrations utilizing just a single mystery key or secret key. In any case, the majority of SSO frameworks require a trusted outsider to take an interest in every user confirmation session. PublicID is a case of a decentralized SSO instrument, which has been generally received by numerous Internet specialist co-ops, for example, Yahoo and Google, with more than 50 000 sites as of now utilizing PublicID as their confirmation conspire. PublicID includes three parts: users, relying partners (RP) or service providers (SP), and identity providers (IdP). In PublicID, an IdP can be likewise a SP and the other way around.

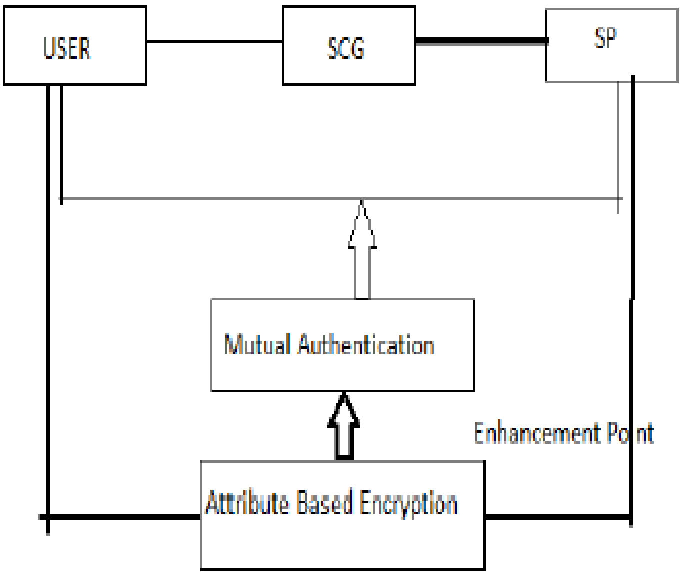
2. Material and Methodology

A. Existing System

In the Existing System in this paper depends on securing the unapproved access of administrations from the non-enrolled users. In this paper RSA algorithm is adjusted with bilinear matching and dynamic nonce age methods to lessen the algorithm cost. In any case, bilinear blending plan contains uncommon hash capacities and hash work is probabilistic and wasteful. Furthermore, in the current framework when mobileuser sends the demand to specialist organizations it will get by all the approved specialist co-op. In the wake of accepting the demand just substantial or closest specialist co-op will satisfy that demand and send reaction to user.

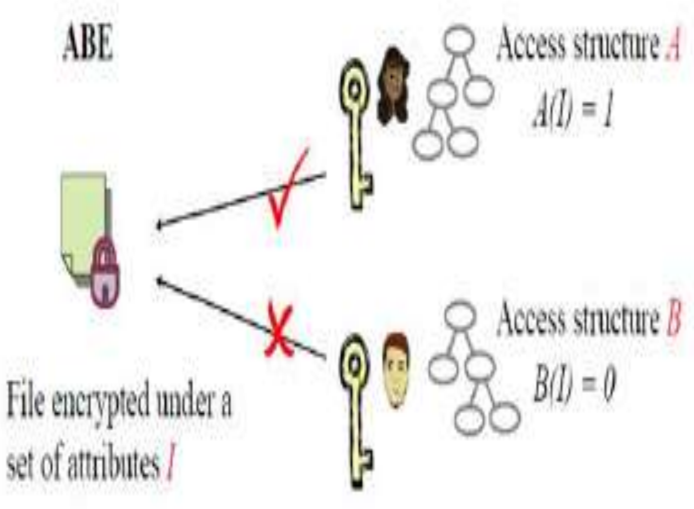
B. Proposed System Architecture

In the existing system the communication is done using mutual authentication. What’s more, for key age bilinear paring with hashing method is utilized however it is exceptionally tedious to encode the entire information to secure the correspondence. So in this paper proposed the new method which decreases the season of key age alongside that give benefits to every user with the assistance of privilege tree.



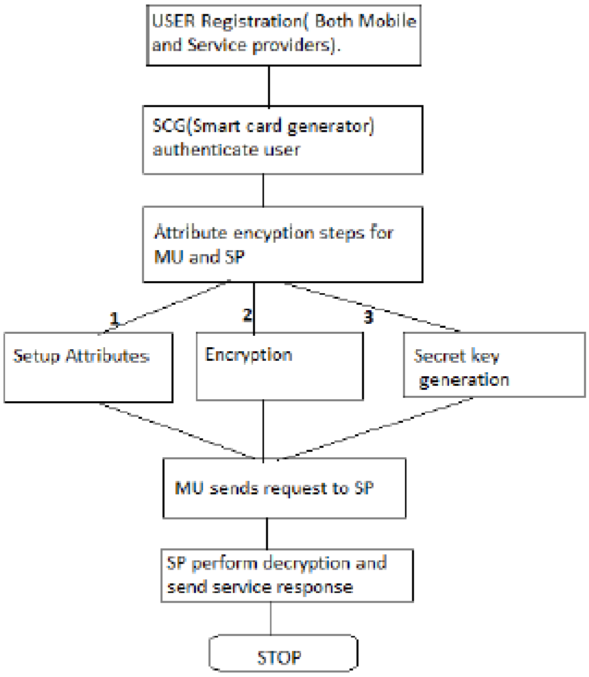
C. Technique

Attribute Based EncryptionABE is a public key cryptography primitive for one-to many communications. In ABE, information is related with attributes for each of which apublic key part is characterized. The encryptor associates the set of attributes to the message by scrambling it with the relating public key segments. Every user is doled out an entrance structure which is typically characterized as an entrance tree over information properties, i.e., inside nodes of the entrance tree are limit entryways and leaf nodes are related with attributes. User secret key is characterized to mirror the entrance structure with the goal that the user can unscramble figure content if and just if the information qualities fulfil his entrance structure. ABE conspire is made out of four algorithms which can be characterized as takes after:



- Setup Attributes
- Encryption
- Secret key generation
- Decryption

D. Process Flow

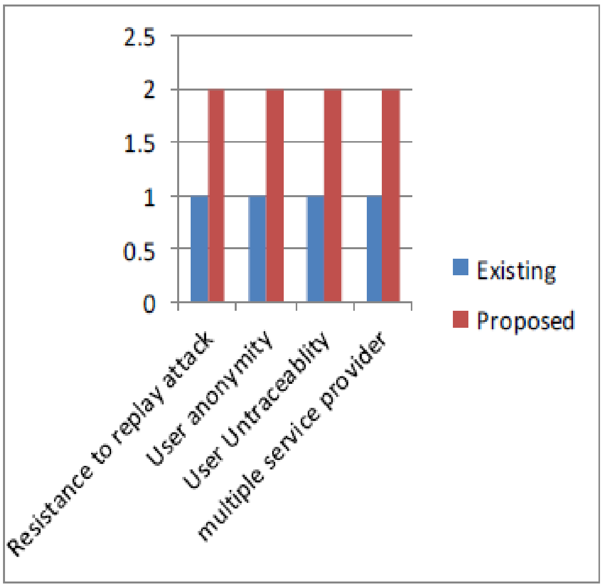

USER Registration(Both Mobile and Service providers).
SCG(Smart card generator) authenticate user
Attribute encyption steps for MU and SP
1
2
3
Setup Attributes
Encryption
Secret key generation
MU sends request to SP
SP perform decryption and send service response
STOP

E. Efficiency of Proposed System

1. The proposed algorithm has proved the best result in terms of execution cost.
2. No data loss.
3. Time complexity to execute the task is very low.
4. Proposed system is more efficient than existing system.
5. Proposed system inherits data dynamics.
6. Our scheme endorses scalable and competent authentication in cloud computing.
7. Proposed scheme are more sheltered and highly competent.

3. Results

As mention above proposed framework is extremely effective than the current framework. The procedure which is utilized as a part of existing framework is extremely tedious and contains high blending operation with hashing. In any case, in our proposed framework which utilizes attribute based encryption spares the key age time and additionally looking time because of this execution is expanded. Proposed framework likewise safeguards the user real identity.



Comparison with Existing System.

4. Conclusion

The use of attribute based encryption method increment the execution of the framework. Quality encryption method gives the user namelessness which implies the personality of user did not uncover. ABS additionally spares the time which is required in bilinear matching for the making of key. ABS creates a standard master key or secret key for communication and the information whatever send from the user isn't scrambled just the property related with that information is encode so it enhances speed of operations. And furthermore Searching of administrations is likewise in view of qualities which gives quicker outcomes than the current framework. In future there can be further developed strategy can be utilized other than attribute based encryption procedure that is KPABE, CP-ABE and so on.

5. References

[1] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, “Location privacy via private proximity testing.” in NDSS. Citeseer, 2011.

[2] A. Thapa, M. Li, S. Salinas, and P. Li, “Asymmetric social proximity based private matching protocols for online social networks,” Parallel and Distributed Systems, IEEE Transactions on, vol. 26, no. 6, pp. 1547– 1559, 2015.

[3] X. Liang, M. Barua, R. Lu, X. Lin, and X. S. Shen, “Healthshare: Achieving secure and privacy-preserving health information sharing through health social networks,” Computer Communications, vol. 35, no. 15, pp. 1910–1920, 2012.

[4] R. Zhang, Y. Zhang, J. Sun, and G. Yan, “Fine-grained private matching for proximity-based mobile social networking,” in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 1969–1977.

[5] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, “Privacy-preserving profile matching for proximity-based mobile social networking,” Selected Areas in Communications, IEEE Journal on, vol. 31, no. 9, pp. 656– 668, 2013.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[7] A. Acquisti, L. Brandimarte, and G. Loewenstein, “Privacy and human behavior in the age of information,” Science, vol. 347, no. 6221, pp. 509–514, 2015.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mhealthcare social network,” Mobile Networks and Applications, vol. 16, no. 6, pp. 683–694, 2011.

[9] M. Von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking,” in IEEE International Conference on Wireless and Mobile Computing. IEEE, 2008, pp. 184–189.

[10] L. Kissner and D. Song, “Privacy-preserving set operations,” in Advances in Cryptology–CRYPTO. Springer, 2005, pp. 241–257.

[11] Q. Ye, H. Wang, and J. Pieprzyk, “Distributed private matching and set operations,” in Information Security Practice and Experience. Springer, 2008, pp. 347–360.

[12] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in Advances in Cryptology-EUROCRYPT. Springer, 2004, pp. 1–19.

[13] E. De Cristofaro and G. Tsudik, “Practical private set intersection protocols with linear complexity,” in Financial Cryptography and Data Security. Springer, 2010, pp. 143–159.

[14]D. Lewis, “icloud data breach: Hacking and celebrity photos,” http://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breachhacking-and-nude celebrity-photos/.

[15] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Nodeaux, and J.-Y. Le Boudec, “Protecting location privacy: optimal strategy against localization attacks,” in Proceedings of the ACM conference on Computer and communications security. ACM, 2012, pp. 617–627.

[16] M. Li, N. Cao, S. Yu, and W. Lou, “Findu: Privacy-preserving personal profile matching in mobile social networks,” in IEEE INFOCOM. IEEE, 2011, pp. 2435–2443.

[17] J. He, M. Dong, K. Ota, M. Fan, and G. Wang, “Netseccc: A scalable and fault-tolerant architecture for cloud computing security,” Peer-toPeer Networking and Applications, vol. 9, no. 1, pp. 67–81, 2016.

[18] M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, “Multicloud-based evacuation services for emergency management,” Cloud Computing, IEEE, vol. 1, no. 4, pp. 50–59, 2014.

ABOUT AUTHORS:

1) K. Sandhya is currently working as an Assistant Professor in Computer Science and Engineering Department, Malla Reddy Institute of Technology & Science, Hyderabad.

2) P. Devika is currently working as an Assistant Professor in Computer Science and Engineering Department, Marri Laxman Reddy Institute of Technology, Hyderabad.