IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-11, Nov 2019 E-ISSN: 2347-2693

A Review on Mutual Authentication and Location Privacy in Mobile Cloud Computing

Karuna Rana[1*], Himanshu Yadav[2], Chetan Agrawal[3]

[1,2,3]Department of Computer Science and Engineering, RITS, Bhopal, India

Corresponding Author: Karuna.rana00@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i11.130134 | Available online at: www.ijcseonline.org

Accepted: 11/Nov/2019, Published: 30/Nov/2019

***Abstract*—** In this paper we have explained about the mobile computing features, limitations which are necessarily should know to us for the future enhancements over the services which are provided by the Cloud Servers (CS). A mobile computing is basically a combination of the cloud computing and the mobile devices whose combination provides us the services over cloud which includes: data storage, data security. Also in this paper our aim is to provide a robust anonymous mutual authentication schemes to provide the effective and the secure data access services to its users. The scheme which used will be helpful to replay attackers and will support creation, modification, to read the information which is put away in the cloud servers. This paper likewise addresses client renouncement. Besides, our verification and access control plot is decentralized and hearty, not at all like different access control plans intended for mists which are incorporated. The correspondence, calculation, and capacity overheads are practically identical to incorporated approaches.

Keywords: Mobile Cloud Computing, Cloud Servers, Security, Smart Cards, Networking.

I. INTRODUCTION

Before sometimes back a user was only capable to talk to each other at a distant. And so it was all sufficient for the purpose of communication. After sometimes it enables users also to take pictures, videos and to save that on their device (locally). But now it is also providing the facility to store the data globally i.e. on Cloud Server (CS). And so the user wishes to take some of the advantages of the cloud services which are strong and quite difficult applications not only for the mobiles, but also for the external sources for example for better power usage and expand storing capacity. So, to take all these facilities on our mobile phones many of the changes have been done till yet in the forms of hardware and networking.

After these changes or modifications, mobile phones still have lack of sources and potential, unsynchronized connection and certain security issues also. To overcome these problems in the mobile phones the concept of the Mobile Cloud Computing has arises in which the Cloud is used as a base (platform) that helps in executing the mobile applications. So, we can say that Mobile Cloud Computing (MCC) includes the storing of data and processing of the data is done outside the mobile devices [1-5].

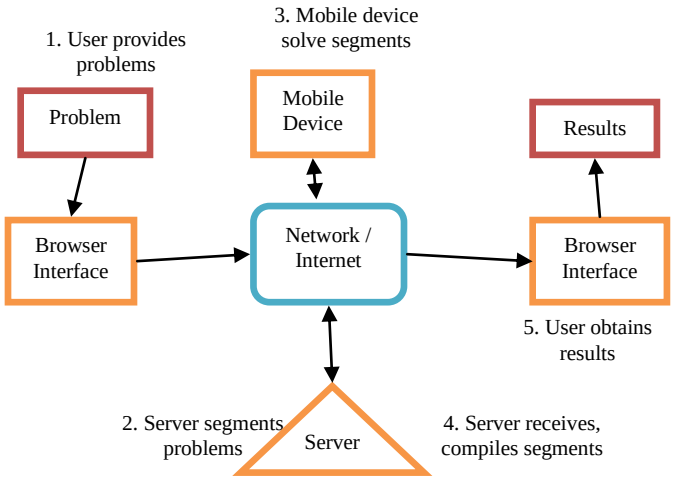

Figure 1: Model of Mobile Computing.

In the above figure we have given an overview of the mobile computing models over server.

1.1 Devices from Mobile Computing

Probably the most well-known kinds of adaptable enlisting contraptions are as given underneath

- Portable PCs, moderate, lightweight units including a full character set reassure and essentially expected as hosts for

programming that may be parameterized, for example, PCs/work areas, PDAs/tablets, and so forth.
- Smart cards that can run different applications yet are commonly utilized for installment travel and verify territory get to.
- Mobile phones, correspondence devices which can call from a partition through cell sorting out development.
- Wearable PCs for the most part compelled to handy keys and on a very basic level expected as joining of programming masters, for instance, arm trimmings, keyless supplements, etc.

1.2 Survey Outline

Section I: In this section explanation of the mobile computing along with devices that come under the mobile computing has been given.
Section II: This section presents the limitations of the cloud computing, along with the contribution of the mobile computing in this paper.
Section III: In this section the comparison of authors with their work has been shown, and how that work existing techniques are related to the present techniques has been shown.
Section IV: This section states the conclusion which is obtained by applying several techniques.

II. LIMITATION IN MOBILE COMPUTING

Range and data transmission Mobile Internet get to is commonly more slow than direct link associations, utilizing advancements, for example, GPRS and EDGE, and all the more as of late 3D and 4G also come in use and the 5G network will be coming soon. Generally, these types of networks are present at a specific range of towers. Since, LANs provides inexpensive network sharing but it has a low speed as compare to others.

• Security standards
As the name it states that in this era of mobile computing where data sharing is about to be done in a thousands of numbers, so to secure that data some security protocols need to be prepared.

• Power consumption
When there is no any source of generation of energy. Thus, mobile devices need to be dependent on the battery power. Depending on the size of the mobile devices. Some may require putting expensive batteries along with the sources.

• Transmission interferences
Temperature may have impact on the mobile phone networks. So, the transmission factors also have an impact over this which needs to be overcome.

• Potential health hazards
The person who uses the mobile phone devices while they are driving may disturb and distract them from their path which is mostly involves in the accidents factors. It may seem to be normal but it should be removed while driving so to reduce the accidents.

• Human interface with device
It is also the severe factor which is responsible with the interference with the mobile phones, because the keyboards and the touch panels are seem to be smaller.

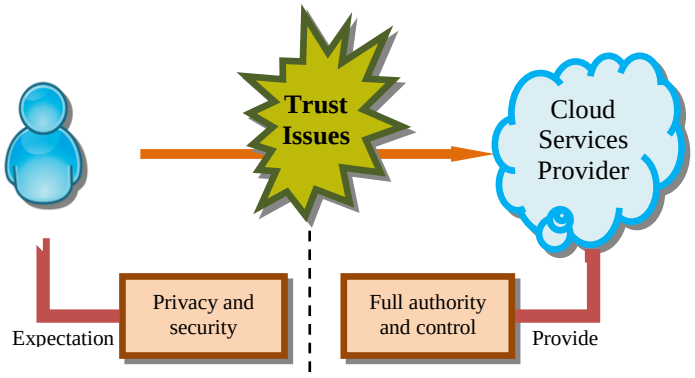

Figure 2: Trust Issues in Mobile Computing.

The above figure 2 shows the trust issues which generally occurs in the mobile computing.

2.1 Contribution

The commitments of this paper are recorded as takes after:
• We propose a brilliant card based strong client validation plot for versatile distributed computing.
• The proposed plot guarantees a portion of the basic properties, for example, utilize secrecy, security against spy, and so on.
• The administration cloud can likewise confine the client from getting a charge out of the pervasive administrations just up to n times, where the estimation of n may change in view of the rule that the cloud client has paid for administrations.
• The thorough formal and also casual security investigation demonstrate that the proposed plan can withstand different known assaults.
• The proposed conspire is assessed utilizing the testbed recreation for its proficiency regarding correspondence and computational expenses.
• The proposed is additionally proficient as far as correspondence, computational and brilliant card data refresh costs when contrasted with other existing plans.

2.2 Current Scenario

As per the discussion of limitations, here are few proposed expected outcome which will present as expected parameters.
1. An implementation and application of cloud process with versatile distributed computing is going to execute. The portable distributed computing will utilize cell phones , its information utilization and shared validation between the

versatile and accessible cloud stage on which authentication hey perform periodically.

2. This is the approach which help preventing users private data leak which is available on mobile devices. The accessing rights and assignments of data which is only required for the process is only processed and prevention of misuse of authentic data can be done.

3. A coordinate transform approach to avoid private location and save physical damage to the mobile cloud user can get performed.

III. LITERATURE SURVEY

Prosanta Gopeand, Ashok Kumar Das [6] In this paper, we intend to propose another powerful unknown shared confirmation plot for versatile cloud condition. Through this plan, both the portable client and the administration cloud need to demonstrate their authenticity, and it in the long run assists the real versatile cloud client with enjoying n times all the pervasive administrations in a protected and productive manner, where the estimation of n may contrast dependent on the main he/she has paid for. The security of the proposed plan is altogether broke down utilizing both formal just as casual security examination. Besides, usefulness and execution correlations utilizing the testbed reenactment among the proposed plan and other existing significant plans uncover that the proposed plan beats other existing plans.

C.Wong et al [7] the plan presented another structure as message which is directly for multicast key overseeing frameworks. The new message structure utilizes one route errands to appropriate crisp key material safely for the clients in the subgroups. The principle advantage of this strategy over the customary message will be sent to standard the clients which part of the significance is planned for them and no extra messages will be sent.

Chen J et al [8] the framework manages decentralized access control structure for the distributed storage techniques, a decentralized access control plans with the mystery key of security protecting extraction. This plan won't require any element validation and synchronization among manys specialists. It takes on the Pedersen confirmation and envelope rules based oblivious affirmation as the fundamental cryptographic natives for tending to the security issues. So the clients get the passwords for the lawful verification components.

Binbusayyis An et al [9] the plan broaden the element of adding personality based client disavowal to convey ABE. The plan additionally accomplishes various free quality specialists. J ganeshkumar et al [10] Decrypting of information can be seen uniquely by a substantial client. This plan averts replay assault which implies overhang dropping can be evaded. Unscrambling of information can be seen uniquely by a legitimate client.

Sushmita Ruj et al [11] this paper gives a framework to check the approval of the message put away in the cloud denied of the client data. It likewise fulfills the protection and client approval. Hwang et al. brought up that if the secret key table is undermined, the entire framework will be uncertain. They at that point proposed another remote client verification plot utilizing keen card. Be that as it may, their plan can't avoid pantomime assault, where a client can imitate the other legitimate client to utilize his/her ID and secret phrase without knowing the mystery key.

Divya bharathy et al [12] the new information is supplanted by the past compose of the deal information even without the arrangement of the earlier information being legitimate. It additionally checks the confirmation of the client and the security approach. A Vijayalakshmi et al [13] this paper deals with the strange endorsement close by an appropriated control procedure for get to. Swetha Maharajanavar et al [14] this paper deals with a system for customer endorsement of the data present in the cloud in a dispersed structure. It gives security measure to the emphasis attack and handles the withdrawal of a customer.

Diffie-Hellman convention is a technique that empowers two clients to share a mystery key and consent to trade the data over unreliable system [15]. This method allows users credential to be transmitted over the network which can cause attack such as Man-in-the-Middle attack. It can also compromise a user's privacy by exposing the users credential without any protection. Password- Authenticated Key Exchange (PAKE) has been introduced by combining key exchange scheme and password-based authentication technique. This scheme uses one-way function to generate verifier and all party involved to compute the secret key. However, this scheme suffers on protecting the verifier from malicious attacker and the corresponding secret password is still needed.

Table 1: Analysis of the Available Recent Algorithms.

Authors	Algorithm/Technique	Advantages	Disadvantages	Remarks
Ashok Kumar Das [1]	Robust anonymous mutual authentication scheme for mobile cloud environment.	Secure and efficient outputs in terms of security.	Security has to suffer sometimes.	Functionality and performance comparisons using the test bed simulation among the

				proposed scheme.
Rescorla E. [15]	Diffie-Hellman protocol.	Enables two clients to share information.	It experiences ensuring the malevolent attackers.	Credentials are the essential point in this.
Swetha Maharajanavar et al [14]	Client approval.	Information is available in the cloud in a dispersed system.	Repetition aggressors.	It gives safety measure to the reiteration assault.
C.Wong et al [7]	New structure as message.	The new message structure utilizes one path undertakings to appropriate crisp key material securely.	It is very slow.	Traditional message will be sent to standard the clients.
Binbusayyis, A. [9]	Decentralized access control structure.	It takes on the Pedersen affirmation and envelope rules based oblivious assurance	It had done the crude cryptography.	The clients get the passwords for the legitimate confirmation components.
Maharajanavar, S. [11]	This uses the methods to check the approval of the messages.	It likewise fulfills the protection and client authorization.	Sometimes the security may impact by the unapproved access.	A new remote client verification plot utilizing keen card.

Cloud computing in mobile learning In traditional m-learning applications [16], all the resources were stored on the server side and learners used to connect to the server via a wireless network to access the resources. Zhao et al. [17] presented the benefits of combining this traditional form of mobile learning with cloud computing to elevate the communication quality. It was possible for a student to communicate with the teacher at any convenient time. A context aware mobile learning system that could be used in mobile computing devices like Tablet PCs and PDAs based on mobile interaction in augmented reality environment was presented [18].

Gai et al. [19] proposed a powerful vitality mindful cloudlet-based versatile distributed computing model (DECM), which concentrated on illuminating the extra vitality utilizations during the remote correspondences. An application-mindful cloudlet determination methodology utilizing in multi-cloudlet situation. As indicated by the application type, when a solicitation originates from a cell phone for offloading an assignment, the most reasonable cloudlet was chosen among different cloudlets.

Machen et al. [20] presented a layered framework which allows a substantial reduction in service downtime and supports containers.

In the comparison table 1 above, some existing recent algorithms are discussed, their advantages, disadvantages, limitation and further extension is discussed in the given table.

IV. CONCLUSION AND FUTURE SCOPE

In this paper we have proposed the decentralized access control technique with the anonymous authentication, which provides users data and prevents from the replay attacks. Since, thousands of the users are storing their information day-to-day on the Cloud Servers and cloud does not even know about it, but it always verifies the user's credentials Key distribution is done in a decentralized way. One limitation is that the cloud knows the entrance arrangement for each record put away in the cloud. In future, we might want to shroud the properties and access strategy of a client.

REFERENCES

[1] M. S. Hwang and L. H. Li, another remote client validation plot utilizing shrewd cards, IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28–30, 2000.

[2] H. Flores and S. N. Srirama, "Versatile cloud middleware," JournalofSystemsandSoftware, http://dx.doi.org/10.1016/j.jss.2013.09.012.

[3] Bellovin S. M. what's more, Merritt M. 1992. Encoded key trade Password-based conventions secure against word reference assaults. In Research in Security and Privacy. pp. 72-84.

[4] National Institute of Standard and Technology. The NIST meaning of distributed computing 2011. Accessible http//www.nist.gov/itl/cloud/transfer/cloud-def-v15.pdf>.

[5] H. T. Dinh, C. Lee, D. Niyato, and P.Wang,A review of versatile distributed computing design, applications, and approaches, Wireless interchanges and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.

[6] Prosanta Gope and Ashok Kumar Das, IEEE Member, Robust Anonymous Mutual Authentication Scheme for n-times Ubiquitous Mobile Cloud Computing Services.

[7] Wong, C. K., Gouda, M., and Lam, S. S. (2000). Secure gathering interchanges utilizing key diagrams. IEEE/ACM exchanges on systems administration, 8(1), 16-30.

[8] Chen, J., and Ma, H. (2014, June). Productive decentralized attributebased get to control for distributed storage with client repudiation. In 2014 IEEE International Conference on Communications (ICC) (pp. 3782-3787). IEEE.

[9] Binbusayyis, An., and Zhang, N. (2015, June). Decentralized attributebased encryption plot with versatile renouncement for sharing information out in the open cloud servers. In Cloud Technologies and Applications (CloudTech), 2015 International Conference on (pp. 1-8). IEEE.

[10] Ganeshkumar, M., and Chow, S. S. (2009, November). Improving protection and security in multi-authority quality based encryption. In Proceedings of the sixteenth ACM meeting on Computer and correspondences security (pp. 121-130). ACM.

[11] Ruj, S., Stojmenovic, M., and Nayak, A. (2014). Decentralized access control with unknown validation of information put away in mists. IEEE exchanges on parallel and appropriated frameworks, 25(2), 384-394.

[12] Bharathy, S. D., and Ramesh, T. (2014). Verifying Data Stored in Clouds Using Privacy Preserving Authenticated Access Control. Proc. IJCSMC, 3(4), 1069-1074.

[13] Vijayalakshmi, An., and Arunapriya, R. (2014). Confirmation of information stockpiling utilizing decentralized access control in mists. Diary of Global Research in Computer Science, 5(9).

[14] Maharajanavar, S. Unknown Authentication of Decentralized Access Control of Data Stored in Cloud. Universal Journal on Recent and Innovation Trends in Computing and Communication ISSN, 2321-8169.

[15] Rescorla E. 1999. Diffie-Hellman key understanding technique.

[16] Leung, Chi-Hong, and Yuen-Yan Chan. "Versatile learning: another worldview in electronic learning." In Advanced learning innovations, 2003. Procedures. The third IEEE global gathering on, pp. 76-80. IEEE, 2003.

[17] Zhao, Weiqing, Yafei Sun, and Lijuan Dai. "Improving PC premise educating through portable correspondence and distributed computing innovation." In Advanced Computer Theory and Engineering (ICACTE), 2010 third International Conference on, vol. 1, pp. V1-452. IEEE, 2010.

[18] Yin, C., David, B. furthermore, Chalon, R., 2009, August. Utilize your portable processing gadgets to learn-Contextual versatile learning framework structure and contextual analyses. In Computer Science and Information Technology, 2009. ICCSIT 2009. second IEEE International Conference on (pp. 440-444). IEEE.

[19] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energyaware cloudlet-based portable distributed computing model for green registering," Journal of Network and Computer Applications, vol. 59, 2016, pp.46-54, doi: http://dx.doi.org/10.1016/j.jnca.2015.05.016.

[20] A. Machen, S. Wang, K. K. Leung, B. J. Ko, and T. Salonidis, "Live Service Migration in Mobile Edge Clouds," IEEE Wireless Communications. Aug. 2017, on the web.

