# HOMOMORPHIC HANDOVER AUTHENTICATION TECHNIQUE FOR MOBILE CLOUD COMPUTING

Gagandeep Kaur, Dr. Gagandeep

*Abstract*— **Mobile Cloud Computing has brought the IT industry to a new level by providing an innovative technique with the help of which one can access anything, anytime from anywhere. It is an industry buzz word since 2009 and a relatively new concept that combines cloud computing, mobile computing and wireless networking. This technology has uplifted the usability experience of mobile users. Over the past few years with huge increase in number of mobile users the requirement of mobile computing technology i.e. cloud computing in mobile devices has also increased enormously. With the gain of popularity in industry this technology faces many challenges in terms of security, bandwidth, mobility, storage capacity, performance, reliability etc. Amongst all these challenges, security challenges remain the prominent one. Secure and efficient handover of mobile nodes is required when mobile nodes move from one access point to the other. The main objective of this paper is to provide efficient and secure homomorphic handover approach to the mobile nodes in cloud environment.**

*Keywords*— **Mobile Cloud Computing (MCC), Security, Handover authentication, Efficiency**

## I. INTRODUCTION

In current scenario human lifestyle is entirely dependent on the devices such as smartphones, PDAs, tablets, laptops etc and with this the entire world is now Mobile-world. The dependence on mobile devices has become more important because of usage of mobile internet leading to useful communication tools. Mobile devices are not bound to a fixed time or place and only this feature of mobile devices provides the rich experience of various services to mobile users. But at the same time there are so many challenges that need to be taken care of while providing these services to users such as mobility, security, battery life, storage, bandwidth [1]. These challenges need to be addressed properly to take the full advantage of mobile devices.

With the huge increase of mobile applications and support provided by cloud computing for the various services for mobile users Mobile Cloud Computing is introduced that integrates Mobile Computing, Cloud Computing and Wireless Networks. Mobile Cloud Computing provides the new features to mobile users by using the advantages of cloud computing to a great extent.

As described earlier, mobile devices are not limited to any place or time thus it is necessary to provide the seamless services to mobile users without any limitation of geographical coverage of access points. For this handover authentication module plays the important role. Therefore it is highly desirable to have an efficient and secure handover protocol.

This paper presents the comprehensive survey of existing handover techniques for the mobile cloud computing and provides a new Multilayered Intrusion Restriction Homomorphic Handover technique. Section II provides a systematic literature survey of the existing handover techniques. Section III provides the proposed dynamic clustering based homomorphic approach for efficient handover. Section IV provides brief information about the actual need of new approach. Section V provides the results for the new implemented approach. Finally, section VI summarizes and concludes this paper.

## II. EXISTING APPROACHES FOR HANDOVER AUTHENTICATION

A secure and efficient authentication scheme for the mobile nodes was proposed by [2]. The key concept used in this approach was use of credentials based on Chameleon hashing. Also Diffie-Hellman key exchange between the mobile node and an access point was used without any communication with authentication server. The advantage of this approach was that it provided a better key exchange and efficient authentication mechanism. But still this was susceptible to man-in-the-middle attack.

A lightweight and provably secure user authentication with anonymity for the global mobility network was proposed by [3]. The key concept in this

approach was use of symmetric cryptography and hash functions. The main advantages of this were prevention from various security attacks, user anonymity, single registration, no password table for user authentication. This approach was also able to defend smart card security breaches.

A universal authentication protocol for privacy preservation for wireless communications was proposed by [4]. This protocol was named as 'Priauth'. The key concept on which this protocol was based was digital group signatures. The major drawback in this was that it was not able to support new group members who join the after system setup. It also lacks in providing single registration property commonly available in most of the existing authentication protocols.

Strong authentication scheme for users in wireless communications that was based on smart cards was proposed by [5]. The key concept of this approach was simple use of symmetric encryption/decryption operations. The major advantages of this approach were its suitability for low-power as well as resource limited mobile devices, ability to defend various security attacks, single registration, no need to maintain any password table and high efficiency.

Further a new approach to overcome the drawbacks of previously defined Priauth protocol mechanism was proposed by [6]. The new technique was related to roaming authentication for wireless and mobile networks. The key concept that was used in this approach was use of conditional privacy preservation mechanism to provide the roaming authentication between two parties.

Pairhand protocol was proposed by [7] for efficient and secure handover authentication. This approach was based on the use of pseudonyms, pairing based cryptography and use of batch signature verification for the privacy preservation. But this Pairhand protocol was having disadvantage in terms of inherent design weakness in the phase of handover authentication. It was also vulnerable to key compromised problem. Further an analysis and improvement of Pairhand protocol was proposed by [8]. A technique to fix the vulnerabilities of Pairhand was proposed in this method.

A secure handover authentication scheme which was based on Ticket based wireless LAN was proposed by [9].This approach was basically an enhancement of the Pairhand protocol mechanism and it reduces the communication and computational overheads during the handover process.

An efficient handover authentication scheme for the wireless networks was proposed by [10]. The key concept used in this approach was use bilinear pairing i.e. this proposed scheme make use of pairing typed cryptography for security of handover process. Batch signature scheme is also used in this approach. The main advantage of it was to defend the security attacks along with reduction in communication and computing costs. The security of it was tested in random oracle model.

A new approach in which a review of the Pairhand protocols family was proposed by [11] and further the security features were enhanced by the method of linearly combining. This approach provided stronger key recovery attack on an improved Pairhand protocol. Further it required fewer signatures to be generated with the same private key.
A new design and analysis of handover authentication scheme for wireless networks based on Chameleon hashing was proposed by [12]. It was the enhanced version of scheme proposed by [2] which was susceptible to man-in-the-middle attack. The main advantages of this were: efficient mutual authentication between mobile node and access point with the use of session key that eliminates the need of storing long term keys by the access point. But still it was having a disadvantage that it was appropriate only for the low power devices in wireless networks.

Efficient and secure authentication scheme for the handover process for 5G Hetnets was proposed by [13]. The basic concept in this approach was use of virtualization of network functions. With the help of network function virtualization the nodes can be considered as homogenous nodes and can be controlled effectively. The advantages of this were: dynamic real time handover, interoperability, scalability and robustness.

Another authentication scheme for mobile devices in the mobile cloud computing was proposed by [14]. This approach was based on service oriented architecture. It was focused on three main aspects of mobile devices such as their limitations, communication quality and application division. But still it can be explored in terms of network independency and application, services sub layers.

An authentication scheme for mobile cloud computing which was based on smart card generator was proposed by [15]. This scheme provided support for mutual authentication, key exchange and the user anonymity. The security strength in this scheme was based on the bilinear pairings and the nonce generation.

Handover authentication for Mobile Cloud Computing with anonymity and untraceability was proposed by [16] which was an improvement over Elliptic Curve Cryptography. This approach was mainly focused on secure key generation using paired key cryptography along with complex hash functions and it was a secure approach but along with this complexity was also increased.

## III. PROPOSED APPROACH

In the proposed work, a homomorphic encryption approach is devised and implemented in which there is the hybridization of key cryptography for effectual handover. During the signal as well as region transformation, there is need to integrate higher degree of integrity and performance. The novel proposed approach is implementing secured hash

approach with Havel based encryption of keys during transmission and authentication at the point of handover. Using this approach, the handover in the mobile cloud based environment becomes integrity and security aware.

In contrast to earlier approach, there may be the merger / mixing of signals because of multiple channels and towers. The proposed homomorphic dynamic clustering based implementation is taking care of layer-wise movement of mobile device and intimate prior to the point of handover. In newly proposed approach at the first instance, a new dynamic key is generated using the randomizers and seed value so that the uniqueness can be maintained. Once a random key is generated, it is passed to the upcoming phases and layers so that security can be enforced at multiple layers. Another phase is encrypting the key generated from previous phase using message digest. Using this approach, a dynamic hash key is obtained which is transferred to other layers to maintain the key integrity and privacy. Encryptions and Strengthening of Security Key by Bit-Stream-Invert -> C2 (It will give same bits in output as in the actual key) and Encryption by SHA (C1 C2). Using this approach the key values are converged to bit stream and finally secured hash algorithm is used. Using this methodology, the final key of will be fully secured with the integration of multiple security layers.

The proposed approach is implemented using following steps:

**1.** Read Mobile Cloud Nodes {MCN[i] such that i<n or i=n}.
**2.** Generation of dynamic graph and framework for movement of nodes in Mobile Cloud environment
**3.** Measure the real time location of each node on the basis of ratio of number of links between and to the location known as border location where handover is required.
**4.** Activate Mobile Cloud Base Station and Satellite with the cluster information.
**5.** Allocation of cluster head on the basis of threshold value.
**6.** The threshold value is to be compared with all nearer mobile cloud sensors and handover point shall be the factor.
**7.** The dynamic clustering of path takes place with the sensing of real time location of mobile device
**8.** Then, the most nearest value to the threshold act as Cluster Head.
**9.** Activation of multilayered hash key in multiple segments depending upon the real time location of mobile device.
**10.** The comparison parameters will be dynamic key generation and exchange in the multiple points to enable secured handover and transmit the signals in secured and integrity aware environment and evaluation of parameters include performance, packets transmission and time factor.

## IV. NEED FOR PROPOSED APPROACH

The classical protocols and algorithms for handover in mobile cloud needs diversified homomorphic encryption based secured as these are single layered because of complexity issue overheads. There is need to integrate the light weight hash algorithm which are prominent and not complex as well. Using this approach of secured hash there will be higher degree of security with very less complexity and execution time. The classical approaches related to security in mobile cloud based handover point do not consider the aspect of key exchange. There is need to design the algorithm in such a way that over all security should not be compromised with the association of minimum overhead. The hash algorithms generate the key string without the issue of interception and malicious traffic. The proposed work will generate the dynamic homomorphic key for secured transmission of data and overall integrity of the network environment.

## V. RESULTS AND DISCUSSIONS

The proposed approach is integration of light weight hash cryptography and dynamic clustering which improves the existing results by reducing the total duration of time that is consumed in the whole process and also step-wise comparison is done for the turnaround time that provides better results. By using this new approach the complexity for the key generation process can be reduced significantly. The graphs showing the comparative analysis for the overall efficiency and turnaround time are as:

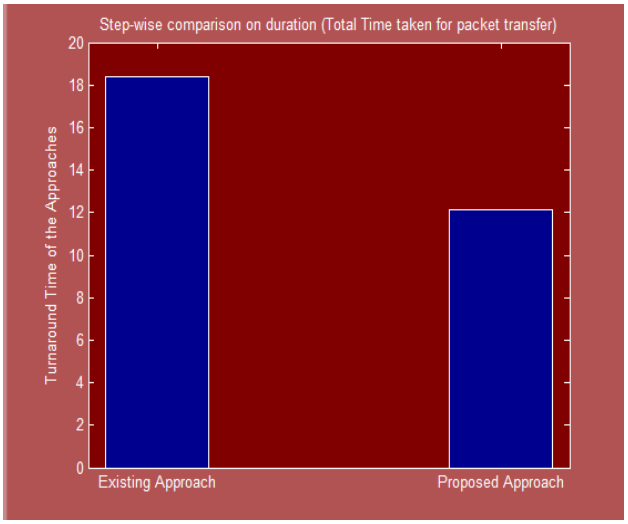


Figure 1. Turnaround Time

Fig.1 shows the step-wise comparison of the duration taken by the earlier approach and the newly proposed approach.
It is evident from the result that the proposed approach helps to reduce the turnaround time for the process. Thus it will enhance the overall efficiency of the process.

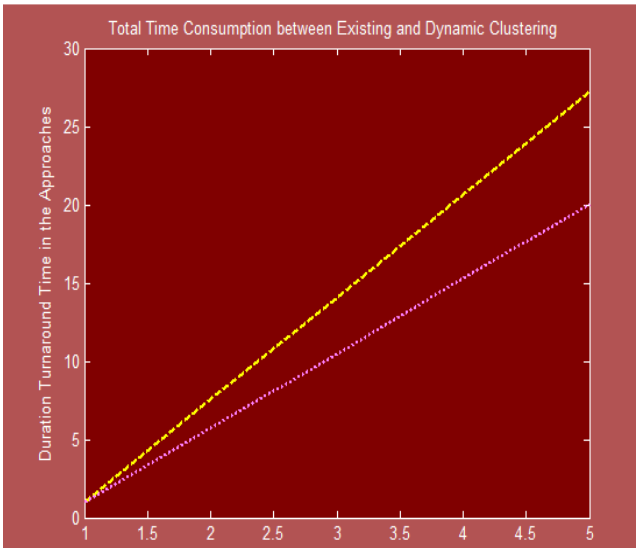


Figure 2. Total Time Consumption

In Fig. 2 the yellow line indicates the total time consumption for the existing approach and other one indicates the time consumption using dynamic clustering. Thus it is evident that dynamic clustering enhances the efficiency.

## VI. CONCLUSION

This paper describes Mobile Cloud Computing which is an active research area because of high usage of mobile devices by large number of users. In Mobile Cloud Computing the handover is one of the main aspects and this paper presents a systematic survey of existing handover techniques. In the existing approaches complexity is still a major factor. Thus a new technique is proposed which is effective in terms of higher integrity, security and performance. The complexity can be reduced using the proposed approach. This approach is implemented for the mobile cloud networks of assorted types but there is scope to implement and test it in other networks and key size can be further reduced using metaheuristic approaches.

## REFERENCES

[1] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, pp. 1587-161, 2013.

[2] J Choi and S Jung, "A Handover Authentication using Credentials Based on Chameleon Hashing," *Journal of IEEE Communication Letter*, vol. 14, no.1,pp. 54-56, 2010.

[3] Chun Chen, Daojing He, Sammy Chan, Jiajun Bu, Yi Gao and Rong Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *International Journal of Communication Systems*, vol. 24, no. 3, pp. 347-362, 2010.

[4] Daojing He, Jiajun Bu, Sammy Chan, Chun Chen and Mingjian Yin,"Privacy Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 431-436, 2011.

[5] Daojing He, Maodema, Yan Zhang , Chun Chen, Jianjun Bu, "Strong User Authentication Scheme with Smart Cards for Wireless Networks," *Special issue of computer communication on information and future communication security*, vol. 34, no. 3, pp.367-374, 2011.

[6] Daojing He, Jiajun Bu, Sammy Chan and Chun Chen, "Strong Roaming Authentication Technique for Wireless and Mobile Networks," *International Journal of Communication systems*, 2012.

[7] Daojing He, Jiajun Bu, Sammy Chan and Chun Chen, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48-53, 2012.

[8] Daojing He, Jiajun Bu, Chun Chen, "Analysis and improvement of a secure and efficient handover authentication for wireless networks," *IEEE Communication Letters*, vol. 16, no. 8, pp. 1270-1273, 2012.

[9] M. Vivek, K.E. Kannammal, "Efficient Hnadover Authentication Scheme for Mobile Nodes in Wireless Networks," *International Journal of Enginnering Research & Technology (IJERT)*, vol. 2, no.1, pp. 1-5, 2013.

[10] Sattar J. Aboud, "Efficient handover authentication scheme using bilinear pairing," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 12, pp. 320-327, 2014.

[11] Weijia Wang and Lei Hu, "A Secure and Efficient Handover Authentication Protocol for Wireless Networks," *Journal of Sensors*, vol. 14, pp. 11379-11394, 2014.

[12] Chin-Chen Chang, Ya-Chieh Huang and Hao-Chuan Tsai, "Design and Analysis of Chameleon Hashing Based Handover Authentication Scheme for Wireless Networks," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 1, pp. 107-116, 2014.

[13] T. Karpagam and S. Sivakumar, "Efficient and Secure Authentication Handover using Network Functions Virtualization," *International Journal of Emerging Technologies in Computer Science & Electronics (IJETCSE)*, vol. 17, no.1, pp. 36-40, 2015.

[14] Muhammad Basit Mujeeb and Muhammad Junaid Arshad, "Mobile Devices Authentication Based on Services Oriented Architecture Using Mobile Cloud Computing," *International Journal of Computer Science and Telecommunications,* vol.7, no. 6, pp. 10-17, 2016.

[15] Shaicy P .Shaji and P. M. Rubesh Anand, "An Effective Scheme for Authentication in Mobile Cloud Computing using Smart Card Generator," *Elysium Journal of Engineering Research and Management*, vol. 3, no. 2, pp. 35-40, 2016.

[16] Xu Yang, Xinyi Huang and Joseph K. Liu, "Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing," *Future Generation Computer Systems,* vol. 62, pp.190-195, 2016.

AUTHORS

**Gagandeep Kaur**, Student of M.Tech, Department of Computer Science, Punjabi University Patiala, Punjab, India.

**Dr. Gagandeep**, Associate Professor, Department of Computer Science, Punjabi University Patiala, Punjab, India