International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue IV, April- 2016

Survey on Authentication Methods and Weight Based Optimized Routing In Mobile Cloud Computing

Ananthanagu U
Assistant Professor, Dept. of CSE
AMC Engineering College,
Bangalore, India
nagu.anantha@gmail.com

Namrata Pattanshetti
M.Tech-Scholar, Dept. of CSE,
AMC Engineering College,
Bangalore, India
namrata.vardhaman@gmail.com

Prerana G Joshi
M.Tech-Scholar, Dept. of CSE,
AMC Engineering College,
Bangalore, India
preranajoshi07@gmail.com

Snigdha Kesh
M.Tech-Scholar,Dept. of CSE
AMC Engineering College
Bangalore, India
snigdha.kesh@gmail.com

Abstract— *Mobile Cloud Computing (MCC) is an emerging technology that attempts to combine the storage and processing resources of cloud environment with dynamicity and accessibility of mobile devices. Security, especially authentication, is fast evolving as focal area in mobile cloud computing research. Application designers and architects use cloud technology advantages to deliver data and information to mobile devices swiftly and seamlessly. However, a critical aspect in this scenario is factor of routing. Complex routing techniques can use up a lot of energy. Coupled with increasing number of cloud data centers, this has the potential to leave a negative impact on our environment. Most existing routing methods involve shortest path routing to ease congestion or traffic in mobile networks. Through this paper, we examine the shortcomings of such existing protocols and discuss mobile base stations and how routing takes place. An algorithm is presented that illustrates the application of the proposed model as presented in this paper. The proposed model is introduced in this work as Weight-Based Optimized Routing. Using this new approach, we can demonstrate a method to lower network congestion or traffic and ensure a more smooth data exchange between mobile devices and cloud nodes. A reduction in mobile network traffic or congestion situations and enhancement of data transmission rates are vital towards achieving a green cloud computing environment. This paper proposes a classification system for existing authentication methods in MCC. The pros and cons of the various methods are discussed.*

Index Terms— Authentication, Base station, Mobile cloud computing, Routing, security, virtualization.

I. INTRODUCTION

Ever since its conception, cloud computing has made big revolution the data storage and data processing. It provides mechanisms to implement it. It implements the on-demand availability of services such as Software, Platform, Infrastructure (through the SaaS, PaaS, IaaS respectively) it gives an good economic solution to meet the ever-fluctuating demand for storage and computational of resources in businesses. In case of mobile cloud computing, the portable and dynamic nature of mobile devices is combined with the scalable resource pooling of cloud computing resources. The computation and communication intensive operations are offloaded to the cloud reduced the mobile device from its inherent limitations. MCC is a computing environment which helps the mobile device to access and compute petabytes of data and execute intensive applications which otherwise would have been not possible due to the limitations of the device. The basic structure of MCC where mobile devices access cloud services via the internet.

As advanced technology, it holds great potential with its fair share of issues, perhaps the most prominent among which is ensuring security and privacy. As in traditional system, authentication holds a important role in security in mobile cloud computing. This paper describes the existing authentication methods in MCC, presents a classification system for the different methods and the advantages and disadvantages of each.

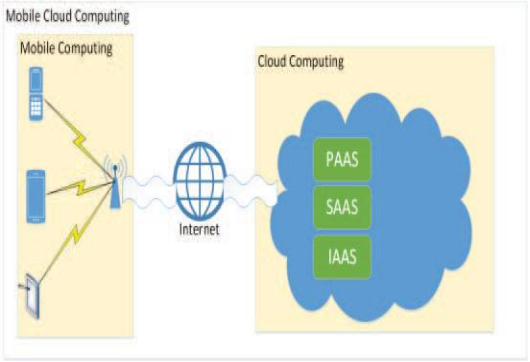


Fig 1. Basic architecture of Mobile Cloud Computing

Mobile cloud computing (MCC) is a combination of cloud computing, wireless networks and mobile telephony. It is a concept which allows streaming of features of mobile applications in a such a way that is gives benefits for mobile device users, service and application providers. Mobile device users have to rely on costly hardware in order to experience good quality applications that may require either extensive

computing performance of beyond the existing capacities which offered by current hardware. Service providers, scale their operational requirements that are based on subscriber base. On other hands, service providers can house their operations in Infrastructure-as-a-Service cloud computing service models. Application developers can choose Platform-as-a-Service services to develop, test, and market their products. In a Software-as-a-Service cloud model, entire software fits and products can be served to users through internet and mobile networks and no need for installing whole software on users' computing devices. The structure of these cloud service models are layered one after the other is constructed in Figure.1

In MCC environment, mobile users use high quality video streaming and software and hence no need to overhead the hardware resources of their mobile devices. In environments like this, mobile networks and cloud computing system interact with each other and offers users an experience that has very good progress, optimized and costs. An example, a mobile game where involving user interface might use CPU cycle and memory, that helps other applications to operate on. Situations which compromise that most users or applications within mobile device, it may reject outright. In cloud computing, huge data processing activities and storage are transfer, minimize hardware upgrade requirements which will be costly. MCC allows an opportunity of decreased heat emissions from mobile devices. Reduced computational loads on mobile device processors will help to lower power consumption. Here, we describe most of the existing research that works on mobile routing. We describe how its an effective on routing can take inter-network congestion. We can explain a routing algorithm which may be used to implement proper communications where a mobile device can be at the intersection of the two different mobile base stations. Routing closely resembles bridging. It shows how an effective routing can not only depend on the shortest distance between two points of nodes, but also gives the shortest path where energy consumption on the base stations and intermediary nodes can be used and optimized.

II. SECURITY IN MOBILE CLOUD COMPUTING

MCC inherits security issues of the cloud computing environment and is limited by its inherent constraints on resources, example- battery life, bandwidth, storage capacity and processing power. This can classify the security issues in MCC into two :- for 1) mobile users and 2) data. Security threats for all mobile applications through malicious code and privacy issues that are related to the location based services and it comes in the first category. Here we describe the security issues for data storage in the clouds such as integrity, authentication and privacy.

A. Security for the Mobile devices

Data and its applications in mobile devices are at high chance to get multiple attacks like virus, Trojan horse etc. We can run antivirus software to continuously observe the file activities for suspected malicious code is not a proper solution in mobile devices due to the resource limitation.

B. Security for Data

1) Privacy

If it's not protected properly then the locations and other private information provided by the users may be accessed and misused by an unauthorized user.

2) Integrity

It's an important feature of the security framework that provides data consistency and protects it from attacker alteration.

3) Authentication

It's the method that confirms the identity of the user who wants to access the resources. It is importance in the mobile cloud computing that we attempt to use few traditional and novel mechanisms for authentication in MCC.

III. SURVEY ON AUTHENTICATION METHODS

This survey encompasses most of the major authentication schemes that are proposed in mobile cloud computing. We discuss the principles behind each authentication methods. Based on the authentication criteria, we have proposed a classification scheme for the surveyed methods. Comparative analysis of methods, highlighting the advantages, disadvantages, implementation stage and future research possibilities are given. In some of surveyed frameworks, two or more methods are used sequentially to strengthen the authentication. Limitations of the mobile devices are listed and feasibility of multi-factor authentication are discussed. Particularly, the effect of a multi-factor authentication on the performance, power consumption, security and privacy are observed and verified. The surveyed authentication methods for mobile cloud computing scenarios can be broadly classified as follows:

1) User profile method
2) Cryptographic method
3) Image-based method
4) Port-knocking method

A. User profile methods

This method makes use of information about the user for identification. Here, 'user' is a generic term; it means either the person using the mobile device or the device itself. User behavioral patterns, biometrics, location information etc. are gathered during a registration phase and verified for authenticated logins.

B. Cryptographic methods

Cryptographic methods are traditionally used for user authentication on different computing platforms. There are many similar methods proposed for mobile cloud computing scenarios. These typically involve exchange of keys or establishment of tickets using a trusted third party and use the same for the establishment of identity.

C. Image-based Methods

This system integrates techniques such as fuzzy vault, picture authentication and zero-knowledge authentication. Here we describe each of these terms to provide background knowledge. In fuzzy vault, secret k is locked with a key A and can be opened by another key B which is "similar" to A. Picture authentication is a visual cryptographic scheme where an image is divided into n transparencies; with any k where k<n the hidden image can be

retrieved, where as with k-1 transparencies a user gain no knowledge about the image or other transparencies. Finally, in zero knowledge system, an entity can prove that he knows a secret without revealing the secret to an observer. A secure channel for communication between the mobile device and server are set up using Diffie-Hellman key exchange algorithm.

D. Port-knocking methods

In port-knocking method, the client sends a no-reply to the closed ports of the server firewall, the synchronized packet. The sequence of ports to which the packets are sent can be selected dynamically or statically. This sequence is logged by server and is the secret key which, when validated opens the appropriate server for port-knocker client.

IV ROUTING OPTIMIZATION METHODS

Our proposed method is primarily directed for proper route selection at mobile network level for the message delivery. And is well recognized, routing forms the crux of mobile communication. Improper routing can set off problems such as jitters, delays, packet drops, etc. in the network. Here we have proposed weight-based route selection algorithm which works off of two fundamental network properties that involves cost of path and channel capacity of the link. Our proposed algorithm, also takes into account selection of base station before the routing calculation and the implementation can take place. In a situation where a mobile device within an area marked as intersection of two base stations, it is becomes necessary to identify the particular base station to which the mobile devices needs to connect. To arrive at a solution, we identify two network factors comprising utility factor and signal strength for the given base station in that particular area. The base station that has a larger weight factor value (W1) will be selected as home base station. The default base station will be considered as the home base station when a mobile device is not in any intersection. In our proposed model, each of the base station would hold a small device called link manager (LM). The LM communicates with Mobile Switching Center to assess and seek various links for transmission between resource manager (RM) and source. LM calculates the weight factor (W2) for different links subject to channel capacity and path cost. The link with the greater weightage factor is selected as optimized route. As might be obvious, in cases where a link is sufficiently free to handle the traffic, the shortest path is selected according to the W2. The RM acts as central database repository for all cloud nodes registered with it. It is responsible for periodically updating the routing table. Transmitting message from mobile device to appropriate resource is the responsibility of RM. Using this proposed method, incidences of network congestion can be significantly reduced. Each and every link can also sufficiently utilized. Optimization of time also takes place as a result.

Calculation of W1

The weight factor W1 is a function of utility and signal strength of a base station. At given particular location, a mobile device is able to compute signal strength of stations that it can reach. Utility is expressed in terms of response provided in a single unit of time (throughput) and the response capacity of a given station. Throughput calculation is given as follows:

Throughput = Response / Unit of time

Thus utility of a base station is gives as

Utility=Throughput / Maximum capacity

Therefore, weight factor (W1) is computed as

Weight Factor (W1) = a*utility + b*signal strength / a +b

("a" & "b" are separate weights factor; where a>b)

Base station with the higher W1 value will be selected as the home base station.

Calculation of W2

Weight factor W2 is dependent on path cost and channel capacity. Path cost corresponds to hop count when negotiating the route from source to destination.

Channel capacity for a different route(C) is given as:

Σ(c1,c2,….cn) / n

Where c1, c2, c3……indicate channel capacities for each link between two consecutive hops.

Weight factor "W2" is computed as:

Weight factor (W2) = c * path cost + d*channel capacity / c+d

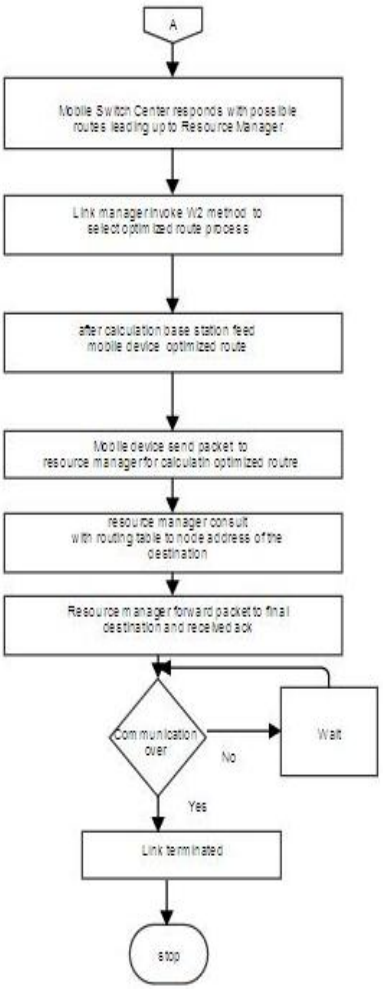
("c" and "b" are different weight factors where d>c).

Route with the maximum W2 value is chosen for data communication.

Algorithm

The algorithm of our proposed model is given as follows:

1. A mobile device begins checking its own location.
2. If it finds its location to be in an intersection formed by two base stations, W1 is called.
3. If otherwise, the only base station detected is set as the home base station.
4. The mobile device transmits a connect request to the base station.
5. The resident LM in that base station sends to the MSC a route request message.
6. The MSC responds with details of all possible routes leading up to the RM.
7. An optimized route selection process using W2 method is invoked by LM.
8. After computation, the base station feeds the mobile device the optimized route calculated.



9. The mobile device transmits the data packet to the RM through the optimized route.
10. In turn, the RM checks the node address of the destination location and begins consulting
its own routing table.
11. Upon locating the appropriate entry, the RM forwards the packet to the final destination
and returns an acknowledgement to the mobile device.
12. The link is terminated when communication is over.

Variable description
BS Base station
MD Mobile device
MSC Mobile switching Center
RM Resource manager
LM Link manager
WI Weight factor regarding base station
W2 Weight factor regarding routing

The mobile cloud computing and networking structure is presented in Figure 2.

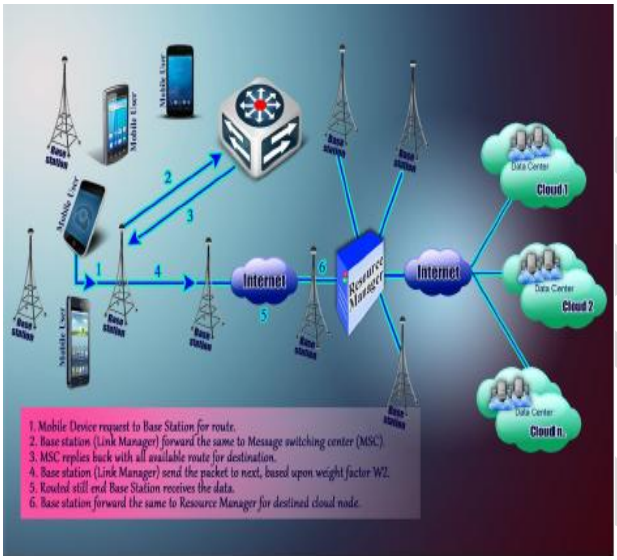
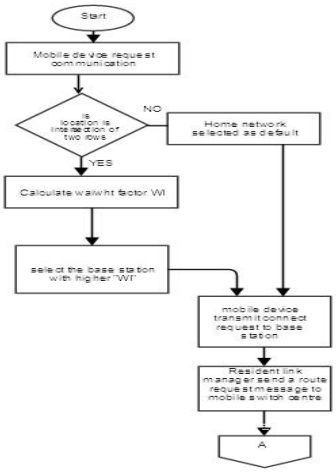


Fig 2. Proposed Network Architecture.

The flowchart for our proposed method is produced below.

Flow chart for the proposed method



V.

CONCLUSION

The advent of smart phones and ubiquitous internet connectivity has heralded a paradigm shift in the computing arena. Mobile devices have become a key platform for computation in the recent years, more so with the emergence of mobile cloud computing. With the storage and data processing offloaded to powerful resources in the cloud, mobile devices are fast overcoming their performance constraints. However, to become a stable and effective computing platform, mobile cloud computing must address several issues, security and privacy chief among them. Particularly, the theoretical and practical aspects of an efficient authentication system in mobile cloud computing is a rapidly developing research focal area of recent times.

REFERENCES

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing – The business perspective," Decision Support Systems, Volume 51, Issue 1, pp. 529-551, April 2011.
[2] International Data Corporation (IDC) Worldwide Quarterly Cloud IT Infrastructure Tracker, "Worldwide Cloud IT Infrastructure Market Growth Expected to Accelerate to 21% in 2015, Driven by Public Cloud Datacenter Expansion, According to IDC," Press Release, 21 April 2015.
[3] A.N. Khan, M.L. Mat Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Future Generation Computer Systems, vol. 29, issue 5, pp. 1278-1299, July 2013.
[4] M. Alizadeh, W. H. Hassan, and T. Khodadadi, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing," 2014 Fifth International Conference on intelligent systems, modelling and simulation (ISMS), pp. 615-618, 27-29 Jan. 2014.
[5] R. Chow et al., "Authentication in the clouds: A framework and its application to mobile users," Proceedings of the 2010 ACM workshop on cloud computing security workshop, pp. 1-6, 2010.
[6] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," HotSec:09: Proceedings of the 4th USENIX workshop on hot topics in security, 2009.
[7] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," Information Security Conference (ISC), 2010.
[8] Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masouka, "TrustCube : An infrastructure that builds trust in client," Future of trust in computing, Proceedings of the first international conference, 2009.
[9] I. Rassan, and H. Shaher, "Securing Mobile Cloud Using Finger Print Authentication", International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 6, pp.41-53, 2013.
[10] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, "Cloud-ready biometric system for mobile security access," Networked Digital Technologies, pp. 192-200, 2012.
[11] D. S. Oh, B. H. Kim, and J. K. Lee, "A study on authentication system using QR code for mobile cloud computing environment," Future Information Technology, pp. 500-507, 2011.
[12] P. S. Teh, B. J. T. Andrew, and Y. Shigang, "A survey of keystroke biometrics," The scientific World Journal, Article ID : 408280, 2013.
[13] M. Choras, and M. Piotr, "Keystroke dynamics for biometric identification," Adaptive and Natural Computing Algorithms, pp. 424-431. Springer Berlin Heidelberg, 2007.
[14] Ahmed E, Gani A, Sookhak M, AbHamid SH, Xia F (2015) Application optimization in mobile cloud computing: Motivation, taxonomies, and open challenges. J Network Comp Appl 52:52–68
[15] Cavdar C (2011) Energy-efficient connection provisioning in WDM optical networks. In: Proceedings IEEE Optical Fiber Communication Conference (OFC), Los Angeles, USA, pp 1–5
[16] Cho B, Gupta I (2010) New algorithms for planning bulk transfer via internet and shipping networks. In: Proceedings IEEE ICDCS, 2010
[17] Cho B, Gupta I (2011) Budget-constrained bulk data transfer via internet and shipping networks. In: Proceedings of ACM ICAC, 2011
[18] Chun BG, Ihm S, Maniatis P, Naik M, Patti A (2011) Clone cloud: elastic execution between mobile device and cloud. In: Proceedings of the Sixth

Conference on Computer Systems, EuroSys'11, ACM, New York, NY, USA, pp 301–314.

[19] Cuervo E, Balasubramanian A, Cho DK, Wolman A, Saroiu S, Chandra R et al (2010) Maui: making smartphones last longer with code offload. In: Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services, MobiSys'10, ACM, New York, NY, USA, pp 49–62.

AUTHORS BIOGRAPHY

Mr. Ananthanagu U, received his Master's degree from Jawaharlal Nehru Technological University, Hyderabad and Bachelor of Engineering from VisvesvarayaTechnological University, Belgavi-Karnataka. He is currently working as a Assistant Professor in the department of CSE in AMC Engineering College, Bengaluru. His areas of research are Cryptography and Big Data Analytics.

Ms. NamrataPattanshetti, Received her Bachelor of Engineering degree from Visvesvaraya Technological University, Belgavi-Karnataka and currently pursuing M.Tech in Computer Science & Engineering from Visvesvaraya Technological University, Belgavi-Karnataka. She has worked as lecturer in colleges affiliated to Jawaharlal Nehru Technological University, Hyderabad and Bangalore University. Her areas of research are Networking, Cloud Computing and Big Data Analytics.

Ms. Prerana G Joshi, received her Bachelor of Engineering degree from Visvesvaraya Technological University, Belgavi-Karnataka and currently pursuing M.Tech in Computer Science & Engineering from Visvesvaraya Technological University, Belgavi -Karnataka. Her areas of research are Networking and Image Processing.

Ms.Snigdha Kesh, received her Bachelor of Engineering degree from West Bengal University of Technology, West Bengal and currently pursuing M.Tech in Computer Science & Engineering from Visvesvaraya Technological University, Belgavi-Karnataka. Her areas of research are networking