2014 Fifth International Conference on Intelligent Systems, Modelling and Simulation

Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing

Mojtaba Alizadeh, Wan Haslina Hassan, Touraj Khodadadi
Malaysian-Japan International Institute of Technology, Universiti Teknologi Malaysia
54100 Kuala Lumpur, Federal Territory, Malaysia
amojtaba2@live.utm.my, wanhaslina@ic.utm.my, ktouraj2@live.utm.my

***Abstract*—Mobile cloud computing is a new computing technology, which provides on-demand resources. Nowadays, this computing paradigm is becoming one the most interesting technology for IT enterprises. The idea of computing and offloading data in cloud computing is utilized to overcome the inherent challenges in mobile computing. This is carried out by utilizing other resource providers besides the mobile device to host the delivery of mobile applications. However, this technology introduces some opportunities as new computing concept, several challenges, including security and privacy are raised from the adoption of this IT paradigm. Authentication plays an important role to mitigate security and privacy issue in the mobile cloud computing. Even some authentication algorithms are proposed for mobile cloud computing, but most of these algorithms designed for traditional computing models, and are not using cloud capabilities. In mobile cloud computing, we access to pooled computation resources and applying more complicated authentication schemes is possible. Using different authentication factors, which is called multi-factor authentication algorithms, has been proposed for various areas. In this paper, feasibility of implementation of different kinds of multi-factor authentication protocols are discussed. Furthermore, the security and privacy of these algorithms are analyzed. Finally, some future directions are recommended.**

Keywords-component; Cloud Computing; Mobile Cloud Computing; Security; Authentication; Multi-factor Authentication

I. INTRODUCTION

In recent years, Cloud computing as a new computing paradigm has been developed very fast. This computing concept became a large scaled IT service model because of fast growth of the number of cloud service providers. Cloud computing offers a standardized access to a large distribution of resources upon demand [1-7]. Furthermore, the development of cloud computing has had a major effect on the information technology industry; major companies like Microsoft, Google and Amazon are working hard to offer more dynamic, dependable and reasonably priced cloud platforms while businesses are trying to remodel their businesses to optimize the advantages of this latest paradigm [8].

The main benefit of cloud computing is the services provided by providers of the cloud service such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) [9, 10]. There are many studies on cloud computing [1, 3, 5, 8, 11-19] that is available; however, the main focus here would be on the potential of cloud computing and the problems arising from this technology [17].

The idea of computing and offloading data in cloud computing is utilized to overcome the inherent challenges in mobile computing. This is carried out by utilizing other resource providers besides the mobile device to host the delivery of mobile applications [17]. In order to offer mobility and ease of use to potential users, mobile cloud computing (MCC) [17, 20-26] has emerged as a subset of cloud computing. MCC is defined as cloud computing services made available in an environment that is mobile. It includes the aspects of cloud computing and mobile networks, thus providing the mobile users with optimal services. In the MCC environment, the mobile device does not require a high configuration such as high memory capacity or high CPU speed because the entire data and complex modules of computing are manipulated in the cloud services [27]. The different parts of mobile cloud computing network is described in Figure 1.

These days, mobile devices are built with features that allow them to access the cloud's resources. The devices are made to easily access the resources due to their portability and ease of use. The mobile devices have two main purposes in MCC. Firstly, the mobile devices serve as the client to retrieve resources out of the cloud since the devices themselves have limited storage and processing capacity thus the use of the cloud. In this case, mobile devices can access to computation and storage resources of cloud service providers. This architecture is the same as the client server architecture. The second purpose of the mobile device is to act the node for the cloud where resources are gathered from all the mobile devices that are participating to solve the problem of processing power and limited storage [20].

Even many technical and business advantages are achieved by organizations using IT resource of cloud computing, but some new security concerns for these organizations are introduced specially for indirect control over sensitive and private data.

Mobile cloud computing encounter to various issues, which are derived from Internet networks and pooled resources in this computing paradigm [28]. Multi-tenancy policy in a cloud requires strong authentication and authorization mechanisms [29, 30].

2166-0662/14 $31.00 © 2014 IEEE
DOI 10.1109/ISMS.2014.111

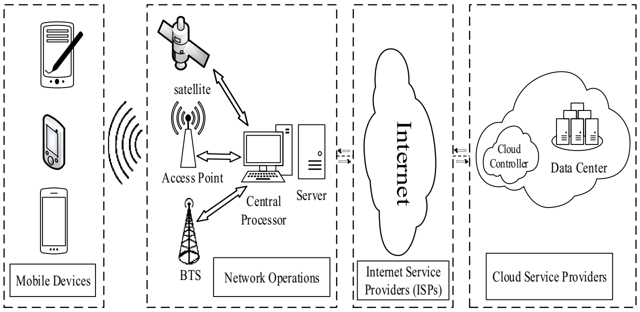

Figure 1: Mobile Cloud Computing Architecture [21]

One of the security protections in IT networks is an authentication. The level of security can be increased using proper authentication method. There are some authentication algorithms, which are proposed to be used in mobile devices. To improve the security of mobile device's users, some researchers recommended adding second factor of authentication [31-36]. In the following part, different kinds of these kinds of algorithms are introduced to get some ideas to use these authentication methods in mobile cloud computing is discussed.

II. AUTHENTICATION FACTORS

To protect user's confidential information, data should be accessible to authenticated people. To gain this aim, various authentication methods are proposed. User authentication can be classified in three different types, including something you know, something you have, and something you are. Each category has different characteristics and implementation methods. The classification is shown in Figure 2.

A. Knowledge-based Authentication

The knowledge-based factor relies on traditional username and password method. This method has been used since the first authentication method invented. Using username and password for user authentication is the most broadly used method among different authentication methods [37]. Even, this method is easy to implement, but there some security vulnerabilities that threats user's security.

The first problem is the difficulty of memorizing passwords for users. This issue resulted in using very simple passwords by users; as a consequence the password can be easily hacked by attackers [38].

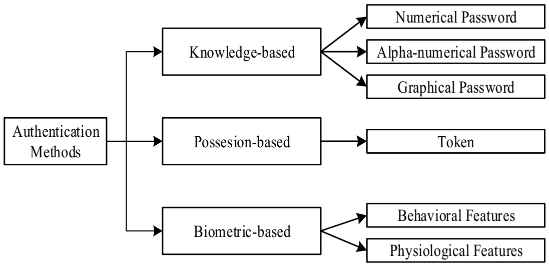

Figure 2: Authentication method classification [39]

Another issue is that passwords are imposing to phishing attacks. An attacker can find user's password and seize the password using different methods like creating a fake web site instead of the real web site.

B. Possession-based Authentication

In this case, a user has some software or hardware token to prove his authentication to the system. These tokens can be valid for on login like One-Time Password [40], or for a special period of time like USB Tokens, Smart Cards, and Public-Key Infrastructure [41].

The most important issue in possession-based authentication is the difficulty and cost of implementation of these authentication methods. To implement this kind of authentication, enough computing resources are needed and as executing an authentication algorithm consumes more energy, it brings some challenges to use this method in mobile devices.

C. Biometric-based Authentication

In Biometric-based authentication method, one of the inherent characteristics of user is used. There some biometric properties that are used to authenticate the user include Fingerprint, Iris, voice, and Face characteristics.

Even these kinds of authentication can provide an acceptable level of security in case of authentication, but the privacy issues are raised by using biometric features. The problem is that if a malicious adversary gets the biometric information of users, an attacker can use these biometric traits because biometric features are not replaceable.

Another issue with this kind of authentication is the cost of implementation. All the mobile devices have not such kind of facilities to recognize biometric characteristics. To implement this kind of authentication, enough computing resources are needed and as executing an authentication algorithm consumes more energy, it brings some challenges to use this method in mobile devices.

III. MULTI-FACTPOR AUTHENTICATION IN MOBILE CLOUD COMPUTING

Different kinds of authentication methods are discussed in the previous part. As mentioned above, each method has some limitations such as privacy, security, performance, and energy. In this part consumption of research, we discuss that how these limitations can be mitigated using mobile cloud computing. We categorized different limitations of authentication methods in three main parts, performance limitations, security, and privacy problem. In following parts, the capability of mobile cloud computing to solve above-mentioned problems using two-factor authentication is discussed.

A. Performance Limitation

In the MCC environment, the cloud offers the general management of the resource for all the mobile devices to assist in going beyond the limits of the devices, specifically data storage and the processing power.

To implement multi-factor authentication methods, we need enough computational resources because more than one authentication method should be processed. The resource limitations in the mobile device can be solved using cloud resources. In MCC, the mobile devices are connected to the cloud computing infrastructure, and process authentication methods; the processing steps are done in the cloud not using mobile device processing power. However, the authentication method should be designed to transfer computational processing to the cloud side. It can be concluded that using multi-factor authentication methods in MCC is reasonable in case of performance.

B. 3.2. Power Consumption

Battery lifetime is one of the major concerns for mobile devices. To improve performance and lower the power consumption some studies have been conducted [42-45], however, most of these works focused on changing the hardware systems of mobile devices. In MCC, there is no need to change mobile device hardware; we can just transfer computing process to the cloud servers, where unlimited resources are available. In summary, the energy consumption of multi-factor authentication methods can be reduced using MCC by transferring computing processes to the cloud servers.

C. Security Issues

Data security is one of the main concerns of MCC users, which can be protected by using proper authentication method. In multi-factor authentication, to improve the security, more than one authentication factors are used to confirm that the person who requests using data is authenticated user. For example, we can use biometric features as a second factor, where ID and password is the first factor, in this case if an attacker finds user's ID and password, she cannot access to the system because her biometric features are not valid. As a conclusion, multi-factor authentication methods are more suitable for MCC environment, where security is an important issue.

D. Privacy Issues

Similar to data security, privacy problems are more concerning issues for MCC users in case of using biometric characteristics as the second factor of authentication. To solve privacy issues in biometric authentication, some solutions are proposed. One of the popular methods for protecting the privacy is encryption, which can be applied to biometrics data. As example, hash function is one of our choices to encrypt data, where the server cannot decrypt it. In MCC, the privacy can be protected using by encrypting the user's data in case of using multi-factor authentication methods.

IV. Conclusion

To protect user's confidential information, data should be accessible to authenticated people. To gain this aim, different authentication methods are proposed. In multi-factor authentication, more than one authentication factor is used. However, this kind of authentication offers better security and privacy, there are some limitations in implementation multi-factor authentication such as processing power and energy-consuming problems for mobile devices. To overcome the limitations of mobile devices such as processing power and battery lifetime, mobile cloud computing has emerged as a subset of cloud computing. In this paper, we discuss some challenges and opportunities of using multi-factor authentication methods, and how mobile cloud computing can mitigate the challenges of using these kinds of authentication methods. As a conclusion, multi-factor authentication is one of the most suitable methods for mobile cloud computing.

V. Acknowledgements

This research is in affiliation with Ministry of Higher Education, Universiti Teknologi Malaysia, Malaysian-Japan International Institute of Technology (MJIIT) and communication System and Network (CSN) research group.

VI. References

[1] A. Verma and S. Kaushal, "Cloud computing security issues and challenges: A survey," in *1st International Conference on Advances in Computing and Communications, ACC 2011, July 22-24, 2011*, Kochi, India, 2011, pp. 445-454.

[2] L. Dung-Hai, L. Dong-Shong, and C. Chun-Pin, "Cloud Computing and Green Management," in *Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on*, 2012, pp. 639-642.

[3] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," pp. 1-32, 2012.

[4] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud Computing: An Overview," in *Cloud Computing*. vol. 5931, M. Jaatun, G. Zhao, and C. Rong, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 626-631.

[5] P. Jain, D. Rane, and S. Patidar, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment," in *2011 World Congress on Information and Communication Technologies, December 11-14, 2011*, Mumbai, India, 2011, pp. 456-461.

[6] L. Guan, X. Ke, M. Song, and J. Song, "A Survey of Research on Mobile Cloud Computing," in *Computer and Information Science (ICIS), 2011 IEEE/ACIS 10th International Conference on*, 2011, pp. 387-392.

[7] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing,* 2011.

[8] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications,* vol. 1, pp. 7-18, 2010.

[9] J. Carolan and S. Gaede, "Introduction to Cloud computing architecture," *SUN Microsystems Inc., pp. 1-40,* 2009.

[10] E. Ghazizadeh, M. Zamani, J.-L. Ab Manan, R. Khaleghparast, and A. Taherian, "A trust based model for federated identity architecture to mitigate identity theft," in *7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, December 10, 2012 - December 12, 2012*, London, United kingdom, 2012, pp. 376-381.

[11] B. P. Rimal, C. Eunmi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," in *Fifth International Joint Conference on INC, IMS and IDC* 2009, pp. 44-51.

[12] J. Xue and J.-J. Zhang, "A brief survey on the security model of cloud computing," in *9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2010, August 10, 2010 - August 12, 2010*, Hong Kong, Hong kong, 2010, pp. 475-478.

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications,* vol. 34, pp. 1-11, 2011.

[14] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments," *Procedia Engineering,* vol. 15, pp. 2852-2856, 2011.

[15] L. M. Vaquero, L. Rodero-Merino, and D. Moran, "Locking the sky: A survey on IaaS cloud security," *Computing (Vienna/New York),* vol. 91, pp. 93-118, 2011.

[16] L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan, and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms," *Computers &amp; Security,* vol. 31, pp. 96-108, 2012.

[17] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generation Computer Systems,* vol. 29, pp. 84-106, 2013.

[18] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems,* vol. 25, pp. 599-616, 2009.

[19] M. Lijun, W. K. Chan, and T. H. Tse, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues," in *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*, 2008, pp. 464-469.

[20] J. Singh, K. S. Mathur, and V. Kumar, "Enhancing Security in Mobile Cloud Computing," *Proceedings of M4D 2012 28-29 February 2012 New Delhi, India,* vol. 28, p. 460, 2012.

[21] M. Alizadeh, W. H. Hassan, N. Behboodian, and S. Karamizadeh, "A Brief Review of Mobile Cloud Computing Opportunities," *Research Notes in Information Science,* vol. 12, pp. 155-160, 2013.

[22] M. Alizadeh and W. Haslina Hassan, "Challenges and Opportunities of Mobile Cloud Computing," presented at the The International Wireless Communications and Mobile Computing Conference, Cagliari, Sardinia, Italy, 2013.

[23] D. Huang, "Mobile cloud computing," *IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter,* 2011.

[24] Q. A. Wang, "Mobile cloud computing," University of Saskatchewan, 2011.

[25] A. Khan and K. K. Ahirwar, "Mobile cloud computing as a future of mobile multimedia database," *International Journal of Computer Science and Communication,* vol. 2, pp. 219-221, 2011.

[26] M. Alizadeh, W. H. Hassan, M. Zamani, and T. Khodadadi, "A Prospective Study of Mobile Cloud Computing," *International Journal of Advanced Computer Technology (IJACT),* vol. 5, pp. 198-210, 2013.

[27] S. K. V. Ko, J. H. Lee, and S. W. Kim, "Mobile Cloud Computing Security Considerations," *Journal of Security Engineering,* vol. 9, 2012.

[28] L. Wentao, "Research on cloud computing security problem and strategy," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, 2012, pp. 1216-1219.

[29] Popovic, x, K., and Z. Hocenski, "Cloud computing security issues and challenges," in *MIPRO, 2010 Proceedings of the 33rd International Convention*, 2010, pp. 344-349.

[30] T. Xiang and A. Bo, "The issues of cloud computing security in high-speed railway," in *Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on*, 2011, pp. 4358-4363.

[31] A. Kemshall, "Why mobile two-factor authentication makes sense," *Network Security,* vol. 2011, pp. 9-12, 2011.

[32] H. Qiangwei, G. Hong, Z. Xiang, and H. Qiang, "Design and implementation of mobile access system based on multi-factor authentication," in *Computer Science and Information Processing (CSIP), 2012 International Conference on*, 2012, pp. 131-134.

[33] C. Kabuya, J. Phiri, and T. Zhao, "Metric Based Technique in Multi-factor Authentication System with Artificial Intelligence Technologies," in *Future Wireless Networks and Information Systems*. vol. 143, Y. Zhang, Ed., ed: Springer Berlin Heidelberg, 2012, pp. 89-97.

[34] H. Al-Assam, H. Sellahewa, and S. Jassim, "On security of multi-factor biometric authentication," in *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for*, 2010, pp. 1-6.

[35] N. D. Sarier, "Practical multi-factor biometric remote authentication," in *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, 2010, pp. 1-6.

[36] F. Hao and D. Clarke, "Security Analysis of a Multi-factor Authenticated Key Exchange Protocol," in *Applied Cryptography and Network Security*. vol. 7341, F. Bao, P. Samarati, and J. Zhou, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 1-11.

[37] I. Jeun, M. Kim, and D. Won, "Enhanced Password-Based User Authentication Using Smart Phone Advances in Grid and Pervasive Computing." vol. 7296, R. Li, J. Cao, and J. Bourgeois, Eds., ed: Springer Berlin / Heidelberg, 2012, pp. 350-360.

[38] E. Ghazizadeh, M. Zamani, J.-L. Ab Manan, and A. Pashang, "A survey on security issues of federated identity in the cloud computing," in *2012 4th IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2012, December 3, 2012 - December 6, 2012*, Taipei, Taiwan, 2012, pp. 562-565.

[39] E. Syta, S. Kurkovsky, and B. Casano, "RFID-Based Authentication Middleware for Mobile Devices," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1-10.

[40] A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud Authentication Based on Anonymous One-Time Password," in *Ubiquitous Information Technologies and Applications*. vol. 214, Y.-H. Han, D.-S. Park, W. Jia, and S.-S. Yeo, Eds., ed: Springer Netherlands, 2013, pp. 423-431.

[41] M. Gharooni, M. Zamani, M. Mansourizadeh, and S. Abdullah, "A confidential RFID model to prevent unauthorized access," in *2011 5th International Conference on Application of Information and Communication Technologies, AICT 2011, October 12, 2011 - October 14, 2011*, Baku, Azerbaijan, 2011.

[42] R. Kakerow, "Low power design methodologies for mobile communication," in *Computer Design: VLSI in Computers and Processors, 2002. Proceedings. 2002 IEEE International Conference on*, 2002, pp. 8-13.

[43] L. D. Paulson, "Low-power chips for high-powered handhelds," *Computer,* vol. 36, pp. 21-23, 2003.

[44] J. W. Davis, "Power benchmark strategy for systems employing power management," in *Electronics and the Environment, 1993., Proceedings of the 1993 IEEE International Symposium on*, 1993, pp. 117-119.

[45] R. Mayo and P. Ranganathan, "Energy Consumption in Mobile Devices: Why Future Systems Need Requirements–Aware Energy Scale-Down," in *Power-Aware Computer Systems*. vol. 3164, B. Falsafi and T. N. VijayKumar, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 26-40.