Journal of Engineering and Applied Sciences 13 (12): 4396-4402, 2018
ISSN: 1816-949X


# Investigation of Security and Privacy Methods for Public Mobile Cloud Computing

[1]Wid Akeel Awadh and [2] Ali Salah Hashim
[1]Department of Computer Information System, [2]Department of Computer Science,
College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

**Abstract:** Mobile cloud computing is a new technology that offers many advantages over the traditional or distrusted information systems. Advantages such as accessibility, availability, reduce the costs of information systems and centralization processes are lead to increase the importance of adopts the mobile cloud computing by the organizations. To gain the full benefits of mobile cloud computing, the public deployment approach would be adopted. The security and privacy challenges of the public mobile cloud computing are still and issues due to data gathering via. wireless network. This study aims to investigate the security and privacy methods that could be utilized to enhance the protections performance of the services and data of public mobile cloud computing. The document analysis based on the systematic review of literature is conducted to address the main aim of this study. The data source of this study is databases of three high impact journals, Science Direct, Web of Science and Scopus. By using systematic taxonomy search on the published articles in last 5 yeasr, 25 related works are retrieved. The findings of this study are constructed based on the critical review of the retrieved related works. The significant results show that the security methods should be utilized at three layers of public mobile cloud computing, cloud layer, wireless connection layer and mobile device layer. The privacy methods are only involve the mobile device layer of public mobile cloud computing. The main security methods of mobile cloud computing are the data encryption, antivirus, firewall, offloading, port-knocking, transfer scheduling, speed data transfer and effective throughput transfer channels. The most useful privacy methods of mobile cloud computing are the QR verification and SMS confirmation. Despite the importance of the security and privacy of mobile cloud computing, to the best of our knowledge, there is not any systematic or comprehensive review were conducted in this domain to clarify the various security and privacy methods based on the architecture of the public mobile cloud computing. This would represent a research contribution. However, the main contribution of this study is the suggested model of the privacy and security of public cloud computing based on the reviewed articles.

**Key words:** Privacy, security, mobile computing, cloud computing, contribution, architecture

## INTRODUCTION

In lasts two decades, the importance of information systems has been increased in various industries such as education, healthcare and commercial (Rehman *et al*., 2017; Mircea and Andreescu, 2011). Information system aims to reduce the expenses and time of accomplish accurate working activities. Thus, the competitive advantage of the organization could be improved. However, the development cost of traditional or distributed information system is expansive due to necessity of develop information system for each department in the organization. On the other hand, the distributed information system may work based on distributed databases which delay the information sending/receiving between the various departments in the organization.

To address the challenges of the distributed information systems, the cloud computing systems were developed. The cloud computing system can be defined as the central technology infrastructure that can be used virtually by all departments in the organization (Liaqat *et al*., 2017). Usually, the virtual technology infrastructure is owned by external party and the organization can reserve a part of these infrastructure based on the business nature of the organization. For example, the organization can reserve 100 GB from the cloud storage. Therefore, the costs of develop the

**Corresponding Author:** Wid Akeel Awadh, Department of Computer Information System,
College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

information systems can be reduced because the organization use the cloud infrastructure rather than develop full insight information system.

Nowadays, Companies such as AMAZON and Google are providing the cloud computing services for the organizations in various industries. The cloud computing services offer many advantages to the organizations such as availability (use the services in any time), centralization (the cloud database can be accessed and updated from the any authentic employee in the organization), reduce the physical expenses of the information system (the storage and processes in the cloud) and reduce the maintaining expenses of the information system (the cloud owner responsible about the maintaining processes) (Avram, 2014).

Mainly, the cloud computing technology classified as three layers: Software as a Service (SaaS) for users or activities, Platform as a Services (PaaS) which the operating system is deployed to manage the information gathering between users and infrastructures and Infrastructure as a Service (IaaS) which include the physical infrastructure of the cloud such as the processor, storage and network (Madni *et al*., 2016).

On the other hand, there are three main deployment approaches of cloud computing (Gustafsson and Orrgren, 2012; Zhang *et al*., 2010): public deployment approach, whereby the cloud infrastructure is fully deployed online by external party, private deployment approach which the cloud infrastructure is constructed in the organization environment and hybrid deployment approach which is mixed between the private and public approaches. The full gained benefits of the cloud computing technology can be addressed through adopt the public deployment approach. However, the main concern of this approach is the data security and privacy. Public cloud computing technology allows the data gathering between the users and the cloud infrastructure using online network, the gathered information may attacked or stolen by strangers. Thus, the data security and security are one of the most important issues of the public cloud computing (Rehman *et al*., 2017).

In last few years, the concept of mobile cloud computing has be defined as the online connection between the users portable devices and the cloud computing infrastructure. Mobile cloud computing provide the accessibility benefit for the users or organization in addition to various cloud computing benefits. By using their mobile devices (such as PDA and smartphone), the users can access the services from anywhere (Saggi and Bhatia, 2015). However, the mobile cloud computing still face the security and privacy challenge (Rehman *et al*., 2017). The wireless connections

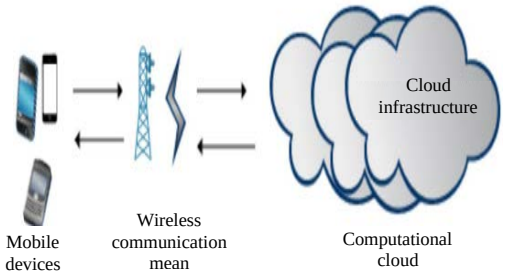


Fig. 1: MCC layers (Akherfi *et al*., 2016)

of mobile cloud computing besides the online gathering of the information increase the possibilities/scenarios of the information attacking much easier.

**Literature review:** Mollah *et al*. (2017) argued that the security of Mobile Cloud Computing (MCC) is about protect the data and services from the attacking while is the privacy is about assure that only the authorized users that can access the data and services. The security and privacy of MCC are integrated to assure the protection performance of the data and services. This section discusses the security and privacy methods that can be utilized to protect the MCC data and services.

The security and privacy methods of MCC would be discussed based on the MCC layer that explained by Akherfi *et al*. (2016) and Donald *et al*. (2013) in Fig. 1a the cloud layer, (Fig. 1b) the wireless connection layer and (Fig. 1c) the mobile devices layer. The attacks on services and data could be happen at the cloud layer which hosts the services and data storages. The attacks on the data could be happen at the connection layer which represents the wireless data transfer channels between the cloud and the mobile. The illegal accessing and data attacks can be happened at the mobile device layer which represents the portable devices that used by the users to accomplish the services. Hence, the security methods involve the three layers of the MCC while the privacy methods involve the mobile layer.

**Security methods of MCC:** As explained in section 2, the security methods are involve the three layers of MCC, cloud, connection and mobile.

At the cloud layer the data encryption is the most useful security methods to protect the services and data from the attacks (Mollah *et al*., 2017). The encryption can be conducted as one stage for all data and services in the cloud storage or use multilevel encryption (such as encrypt the services and data of each organization separately, before re-encrypt all data in the public cloud storage). The encryption methods that can be used in

MCC are the watermark (for images), symmetric, asymmetric (for text) and steganography (for various format).

Anwar *et al.* (2017) suggested the encryption based virtual MCC storages to increase the difficulty of data attacking. This method is based on segment the cloud into many virtual machines and storages and the encryption of each virtual part is conducted separately of other parts. Hence, the data encryption will be more effective and faster and the attacker tries will not success to attack the overall data and services in the cloud.

Liaqat *et al.* (2017) explained that the encryption of data and services of public MCC is costly either time or money costs. Thus, the classifications of the data services in the cloud will reduce the volume of the data that need to be encrypted. On the other hand, the data and services classification will increase the security performance through give the opportunity to select fixable security methods for less data volume. The classification is based on classify the data and services as private and public data. Hence, the public data not require security processes while the security efforts should be focused on the private data and services.

Another security method at the cloud layer called offloading is presented by Bhattacharya and De (2017), Vaezpour *et al.* (2016), Shaukat *et al.* (2016), Shuja *et al.* (2016) and Akherfi *et al.* (2016). In this method, the users can gather the data using internal wireless connection with server inside the organization (offline), before gather the data between the internal server and the cloud using wire connections, i.e., the wire connection is more secure than the wireless. In addition to offloading method (Singh and Chatterjee, 2017) suggests many security methods for the cloud layer of MCC: firewall and antivirus to prevent the threats, data and services encryption and define the signatures, i.e., the allowed devices to access the cloud services and data.

Furthermore, Hashem *et al.* (2015) proposed the data transfer of MCC through secure tools (third party). The "Hadoop/MapReduce" is one of the most secure tools which installed on the local server of the organization and conduct the data transfer based on two stages, receive/send the data from/to users using local wireless connections and receive/send data from/to cloud using wire connection. The Hadoop/MapReduce tool is effective for big data transfer because it offer secure transfer channels of large bandwidths to accomplish the data transfer in short time. However, researchers such as Akherfi *et al.* (2016) and Singh and Chatterjee (2017) are not recommended the third party of data transfer due to expenses of the required requirements.

Khan *et al.* (2013, 2017) proposed a security method for cloud and wireless connection layers and this method called "port-knocking". The "port-knocking" is based on the strategy of define the authentication of the devices that can accessed the MCC connection and gather the information with the cloud. Hence, the devices the authorized IP should defined in advance and the undefined or strange IPs connections will be refused.

At the wireless connection layer (Ahmed *et al.*, 2015a, b) mentioned that the security of MCC is affected by the data transfer speed and throughput. The low transfer speed and the routing of transfer due to low throughput are increasing the opportunities to attack the hold data in the connection channels. Thus, it is necessary to use effective speeds and throughout to transfer the data. Methods such as optic fiber connection would be effective to protect the transferred data through reduce the hold data in the wireless connection channels. Another method is offloading data transfer techniques, which explained in the above by Akherfi *et al.* (2016)' study.

Similar to Ahmed *et al.* (2015a, b), the studies by Gani *et al.* (2014) and Liu *et al.* (2015) focused on improve the MCC security at connection layer through reduce the hold data in the wireless network between the cloud and the mobile device. A transfer technique called seamless connectivity is proposed to divide the transferred data into small block, each block can be transferred via different network paths depend on the available paths (to avoid the traffic) and the data blocks would be merged at the destination level. Hence, the traffic of data transfer will be avoided and the attackers cannot benefit from the attacking of small data blocks, i.e., the small data blocks are not serviceable. In the same context (Ghomi *et al.*, 2017) proposed a load balancing algorithm to balance the transfer data the MCC data via. the available wireless network paths in order to avoid the network overload. The load balancing method is depend on reserve the transfer paths before transfer the data to assure that the data will be delivered without any hold in the wireless connection. Moreover, Madni *et al.* (2016) and Aslam *et al.* (2017) proposed the scheduling of data transfer to avoid the overload on the wireless network. The scheduling is depend on evaluate the available resources of the network and manage the data transfer based on the available paths. The scheduling may be conducted based on the time, data importance or data size.

At the mobile device layer, Ibukun and Daramola (2015) argued that the antivirus is one of the most important methods to detect the threats is that could attack the mobile devices. The antivirus application

should be suitable for mobiles (mobile specification). Most antivirus providers like kaspersky produce suitable versions for mobiles devices.

**Privacy methods of MCC:** The privacy methods of MCC involve the mobile layer (user side). Rassan and Al Shaher (2013) focused on the authentication access of cloud computing using user's mobiles. Rassan and Al Shaher (2013) mentioned that the traditional authentication methods based on usernames and passwords has many drawbacks like the ability of own or stolen user's identification by other users. The fingerprint could be effective method to verify the legal accessing of users accounts due to difficulty of stole the fingerprint of any person.

Abolfazli *et al.* (2014) mentioned that the privacy methods such as voice and face recognitions are required advance requirements which may not available in all mobile devices. Thus, the accounts accessing using traditional passwords would be effective for all users. However, the users should be forced to assign strong passwords, i.e., letters, numbers and special characters in order to increase the difficulty of the illegal accessing.

Sookhak *et al.* (2014) and Stajano *et al.* (2014) explained that one of the most known illegal accessing of MCC is conducted by computerized applications that try to guess the users passwords using automatic counters. To address this problem, the cloud can send challenge questions that can be answered only by the human in order or assure that the sign in process is done by a person.

Sun *et al.* (2015) sees that account accessing using passwords may be weak if the passwords stole or known by strangers. However, the password accessing is flexible methods due to low requirement to verify the accounts authentication using text passwords. Therefore, it is important to prevent the strangers form stole or attack the user's password. Sun *et al.* (2015) argued that the encryption of user's passwords could enhance the effectiveness of user's privacy. The encryption of user's passwords increases the difficulty of attack the gathered passwords via MCC.

Alizadeh *et al.* (2016) argued that there is various privacy methods could be utilized for MCC to assure the users authentication, access the service using username and password, accessing using biometric identification, i.e., voice or face recognition, accessing thorough valid QR, accessing through confirm SMS code and analyze the trust of the account through approaches such as analyze the recent used device to access the account. The critical review of Alizadeh *et al.* (2016) founded that the biometric passwords such as voice recognition and the SMS verification are the most useful privacy methods of MCC based on many factors like the methods cost, technology requirements and privacy level. It is necessary to mentioned that the biometric signature or the number of mobile devices should be stored in the cloud at the signup stage for the purpose of next verifications.

## MATERIALS AND METHODS

The main purpose of this study is to investigate the security and privacy methods that can be utilized to improve the security performance of mobile cloud computing. For this purpose, the document analysis method of the past studies is conducted. The data source is the review and research articles that published in the last 5 years in three high impact databases, science direct, web of science and Scopus. The researcher uses the following taxonomy search queries in order to filter the related studies:

("Cloud computing" or "cloud" and "mobile computing" or "mobile application" or "mobile cloud computing" and "security" and "privacy").

The retrieved articles from the three databases are filtered and the redundant articles are avoided. Thus, the final number of the retrieved articles is 25 which explained in the literature review. Based on the searching taxonomy results, it can be noticed that there is limitation in the conducted works in the security and privacy issues of the mobile cloud computing domain. Thus, this study could be important to support the researching in this domain.

## RESULTS AND DISCUSSION

The reviewed articles based on the research method show that there are several methods can be adopted to enhance the security and privacy performance of the MCC. Table 1 summarizes the security methods of the MCC. It can be noticed that the data encryption of the data and services is important security methods at the cloud layer. The classification of services and data as public and private classes would reduce the cost of data encryption. Also, the data transfer based on offloading would be effective to enhance the security level of the MCC. The researchers not recommend the offloading using third party tools. Other important security methods at the cloud layer are the firewall and antivirus. On the other hand, methods such as port-knocking could be effective to improve the security of MCC at cloud and wireless connection layers. Furthermore, the data transfer speed, effective throughput, seamless connectivity and

Table 1: Summary of security methods of MCC

| Sources | Data encryption | Offloading | Offloading (third party) | Firewall | Antivirus | Port-knocking | Speed and effective transfer | Seamless connectivity | Transfer scheduling |
|---|---|---|---|---|---|---|---|---|---|
| Mollah *et al.* (2017) | ✓ | X | X | X | X | X | X | X | X |
| Anwar *et al.* (2017) | ✓ | X | X | X | X | X | X | X | X |
| Liaqat *et al.* (2017) | ✓ | X | X | X | X | X | X | X | X |
| Bhattacharya and De (2017) | X | ✓ | X | X | X | X | X | X | X |
| Singh and Chatterjee (2017) | ✓ | ✓ | X | ✓ | ✓ | ✓ | X | X | X |
| Khan *et al.* (2017) | X | X | X | X | X | ✓ | X | X | |
| Aslam *et al.* (2017) | X | X | X | X | X | X | X | X | ✓ |
| Madni *et al.* (2016) | X | X | X | X | X | X | X | X | ✓ |
| Vaezpour *et al.* (2016) | X | ✓ | X | X | X | X | X | X | X |
| Shaukat *et al.* (2016) | X | ✓ | X | X | X | X | X | X | X |
| Shuja *et al.* (2016) | X | ✓ | X | X | X | X | X | X | X |
| Akherfi *et al.* (2016) | X | ✓ | X | X | X | X | X | X | X |
| Abaker *et al.* (2015) | X | X | ✓ | X | X | X | X | X | X |
| Ahmed *et al.* (2015a) | X | X | X | X | X | X | ✓ | X | X |
| Ahmed *et al.* (2015b) | X | X | X | X | X | X | ✓ | X | X |
| Ibukun and Daramola (2015) | X | X | X | X | ✓ | X | ✓ | X | X |
| Liu *et al.* (2015) | X | X | X | X | X | X | X | ✓ | ✓ |
| Gani *et al.* (2014) | X | X | X | X | X | X | X | ✓ | ✓ |
| Khan *et al.* (2013) | X | X | X | X | X | ✓ | X | X | X |

Table 2: Summary of privacy methods of MCC

| Sources | Strong text passwords | Encrypt password | Fingerprint | Voice recognition | Face recognition | QR verification | SMS confirmation | Challenge questions |
|---|---|---|---|---|---|---|---|---|
| Alizadeh *et al.* (2016) | X | X | X | ✓ | ✓ | ✓ | ✓ | X |
| Wang *et al.* (2015) | X | ✓ | X | X | X | X | X | X |
| Sookhak *et al.* (2014) | X | X | X | X | X | X | X | ✓ |
| Stajano *et al.* (2014) | X | X | X | X | X | X | X | ✓ |
| Abolfazli *et al.* (2014) | ✓ | X | X | X | X | X | X | X |
| Rassan and Al Shaher (2013) | X | X | ✓ | X | X | X | X | X |

transfer scheduling approaches are effective to reduce the hold data on the wireless connection which not give the opportunity to attack the data at the connection layer. In addition, the antivirus on the user's mobiles would prevent the threats attacks from attack the data at the mobile device layer.

Table 2 summarizes the privacy methods of the MCC. It can be noticed that the privacy methods are involve the mobile device layer. Some researchers prefer the accounts accessing using strong text password due to low requirements of this method. Other researchers prefer the biometric accessing methods such as fingerprints, voice recognition and face recognition due to powerful of these methods in define the legal accessing for MCC services. The QR and SMS confirmations are effective to define the legal accessing without the need to advance technologies. The challenge questions is used usually to prevent the computer machines from trying to access the uses account illegally using techniques such as automatic counters of IDs.

Based on Table 1 and 2, the suggested security and privacy model of MCC is presented in Fig. 2. For effective security of MCC, the data and services encryption at the cloud level should be conducted. In order or reduce the encryption costs, the data and services need to classified as public and private classes. The private data and services are required to be encrypted while the public services and data will not be encrypted. The antivirus and firewall are other security methods that must be utilized ate the cloud level of MCC. At the wireless connection layer, it is important the security performance of MCC

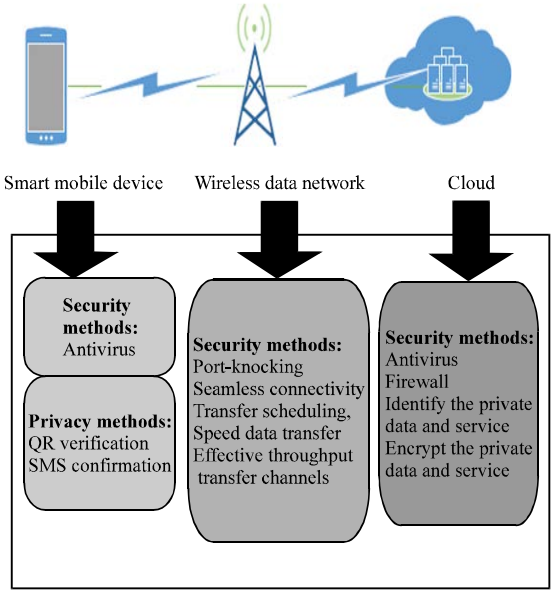


Fig. 2: Proposed security and privacy model of MCC

through many methods such as port-knocking, seamless connectivity, transfer scheduling, speed data transfer and effective throughput transfer channels. Lastly, at the mobile device layer, the antivirus should be installed by the users to improve the security level of the MCC while methods such as SMS confirmation and QR verification are useful to enhance the privacy performance of the MCC without the need to apply advance technology.

## CONCLUSION

This study reviews the security and privacy methods that could be utilized to enhance the protection performance of the public MCC. The systematic review is conducted to address the main aim of this study. The searching method found that in the last 5 years, there are 25 published articles in high impact journals that related to the security and privacy of MCC. The reviewed security and privacy methods of the MCC are classified based on the three main layers of the public MCC, cloud layer, wireless connection layer and the mobile device layer. The most useful security and privacy methods are structured as proposed model of the public MCC security.

## RECOMMENDATIONS

In the future further research could be conducted based on the baselines of this study. The most suitable encryption methods of MCC could be analyzed critically, the analyses of the privacy methods of MCC would be expanded and the offloading transfer method need to be explained in detail.

## REFERENCES


Abolfazli, S., Z. Sanaei, A. Gani, F. Xia and L.T. Yang, 2014. Rich mobile applications: Genesis, taxonomy and open issues. J. Netw. Comput. Appl., 40: 345-362.

Ahmed, E., A. Gani, M. Sookhak, S.H.A. Hamid and F. Xia, 2015a. Application optimization in mobile cloud computing: Motivation, taxonomies and open challenges. J. Netw. Comput. Appl., 52: 52-68.

Ahmed, E., A. Gani, M.K. Khan, R. Buyya and S.U. Khan, 2015b. Seamless application execution in mobile cloud computing: Motivation, taxonomy and open challenges. J. Netw. Comput. Appl., 52: 154-172.

Akherfi, K., M. Gerndt and H. Harroud, 2016. Mobile cloud computing for computation offloading: Issues and challenges. Appl. Comput. Inf., 14: 1-16.

Alizadeh, M., S. Abolfazli, M. Zamani, S. Baharun and K. Sakurai, 2016. Authentication in mobile cloud computing: A survey. J. Network Comput. Appl., 61: 59-80.

Anwar, S., Z. Inayat, M.F. Zolkipli, J.M. Zain and A. Gani *et al*., 2017. Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey. J. Netw. Comput. Appl., 93: 259-279.

Aslam, S., S.U. Islam, A. Khan, M. Ahmed and A. Akhundzada *et al*., 2017. Information collection centric techniques for cloud resource management: Taxonomy, analysis and challenges. J. Netw. Comput. Appl., 100: 80-94.

Avram, M.G., 2014. Advantages and challenges of adopting cloud computing from an enterprise perspective. Proc. Technol., 12: 529-534.

Bhattacharya, A. and P. De, 2017. A survey of adaptation techniques in computation offloading. J. Netw. Comput. Appl., 78: 97-115.

Donald, A.C., S.A. Oli and L. Arockiam, 2013. Mobile cloud security issues and challenges: A perspective. Intl. J. Electron. Inf. Technol., 3: 1-6.

Gani, A., G.M. Nayeem, M. Shiraz, M. Sookhak and M. Whaiduzzaman *et al*., 2014. A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing. J. Netw. Comput. Appl., 43: 84-102.

Ghomi, E.J., A.M. Rahmani and N.N. Qader, 2017. Load-balancing algorithms in cloud computing: A survey. J. Netw. Comput. Appl., 88: 50-71.

Gustafsson, B. and A. Orrgren, 2012. Cloud computing: The adoption of cloud computing for small and medium enterprises. BA Thesis, Jonkoping University, Jonkoping, Sweden.

Hashem, I.A.T., I. Yaqoob, N.B. Anuar, S. Mokhtar and A. Gani *et al*., 2015. The rise of big data on cloud computing: Review and open research issues. Inf. Syst., 47: 98-115.

Ibukun, E. and O. Daramola, 2015. A systematic literature review of mobile cloud computing. Intl. J. Multimedia Ubiquitous Eng., 10: 135-152.

Khan, M.A., M.M. Rahman, M. Tania, N.F. Shoshee and A. Xu *et al*., 2013. Antioxidative Potential of Duranta Repens (Linn.) Fruits Against H2O2 Induced Cell Death In Vitro. Afr. J. Traditional Complementary Altern. Med., 10: 436-441.

Khan, S., M. Shiraz, L. Boroumand, A. Gani and M.K. Khan, 2017. Towards port-knocking authentication methods for mobile cloud computing. J. Netw. Comput. Appl., 97: 66-78.

Liaqat, M., V. Chang, A. Gani, S.H.A. Hamid and M. Toseef *et al*., 2017. Federated cloud resource management: Review and discussion. J. Netw. Comput. Appl., 77: 87-105.

Liu, J., E. Ahmed, M. Shiraz, A. Gani and R. Buyya *et al*., 2015. Application partitioning algorithms in mobile cloud computing: Taxonomy, review and future directions. J. Network Comput. Appl., 48: 99-117.

Madni, S.H.H., M.S.A. Latiff and Y. Coulibaly, 2016. Resource scheduling for Infrastructure as a Service (IaaS) in cloud computing: Challenges and opportunities. J. Netw. Comput. Appl., 68: 173-200.

Mircea, M. and A.I. Andreescu, 2011. Using cloud computing in higher education: A strategy to improve agility in the current financial crisis. Commun. IBIMA., 2011: 1-15.

Mollah, M.B., M.A.K. Azad and A. Vasilakos, 2017. Security and privacy challenges in mobile cloud computing: Survey and way ahead. J. Netw. Comput. Appl., 84: 38-54.

Rassan, I.A. and H. Al Shaher, 2013. Securing mobile cloud using finger print authentication. Intl. J. Netw. Secur. Its Appl., 5: 41-53.

Rehman, M.H.U., C.S. Liew, T.Y. Wah and M.K. Khan, 2017. Towards next-generation heterogeneous mobile data stream mining applications: Opportunities, challenges and future research directions. J. Netw. Comput. Appl., 79: 1-24.

Saggi, M.K. and A.S. Bhatia, 2015. A review on mobile cloud computing: Issues, challenges and solutions. Intl. J. Adv. Res. Comput. Commun. Eng., 4: 29-34.

Shaukat, U., E. Ahmed, Z. Anwar and F. Xia, 2016. Cloudlet deployment in local wireless networks: Motivation, architectures, applications and open challenges. J. Netw. Comput. Appl., 62: 18-40.

Shuja, J., A. Gani, M.H.U. Rehman, E. Ahmed and S.A. Madani *et al*., 2016. Towards native code offloading based MCC frameworks for multimedia applications: A survey. J. Netw. Comput. Appl., 75: 335-354.

Singh, A. and K. Chatterjee, 2017. Cloud security issues and challenges: A survey. J. Netw. Comput. Appl., 79: 88-115.

Sookhak, M., H. Talebian, E. Ahmed, A. Gani and M.K. Khan, 2014. A review on remote data auditing in single cloud server: Taxonomy and open issues. J. Network Comput. Appl., 43: 121-141.

Stajano, F., M. Spencer, G. Jenkinson and Q. Stafford-Fraser, 2014. Password-Manager Friendly (PMF): Semantic annotations to improve the effectiveness of password managers. Proceedings of the 2014 International Conference on Passwords, December 8-10, 2014, Springer, Trondheim, Norway, ISBN:978-3-319-24191-3, pp: 61-73.

Sun, H., K. Sun, Y. Wang and J. Jing, 2015. Trustotp: Transforming smartphones into secure one-time password tokens. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, October 12-16, 2015, ACM, Denver, Colorado, USA., ISBN:978-1-4503-3832-5, pp: 976-988.

Vaezpour, S.Y., R. Zhang, K. Wu, J. Wang and G.C. Shoja, 2016. A new approach to mitigating security risks of phone clone co-location over mobile clouds. J. Netw. Comput. Appl., 62: 171-184.

Zhang, Q., L. Cheng and R. Boutaba, 2010. Cloud computing: State-of-the-art and research challenges. J. Internet Serv. Applic., 1: 7-18.