Global Regional Review (GRR)
URL: http://dx.doi.org/10.31703/grr.2019(IV-I).18

Challenges of Confidentiality and Security in Mobile Cloud Computing and Protective Measures

Vol. IV, **No.** I (Winter 2019) | **Page:** 154 – 163 | **DOI:** 10.31703/grr.2019(IV-I).18

p- ISSN: 2616-955X | **e-ISSN:** 2663-7030 | **ISSN-L:** 2616-955X

Dost Muhammad Khan[*] | Tariq Aziz Rao[†] | Faisal Shahzad[‡]

Abstract *Mobile Cloud Computing (MCC) has a significant potential to provide scalability, reliability, extra battery life, and additional storage capacity. Due to the flexible infrastructure and simplicity of access, cloud computing has become widespread. Energy consumption and execution time have also considerably enhanced by shifting the execution of resources consuming tasks that bring the benefit to mobile users. However, security and privacy is the major barrier to this growing trend of computing aptitude. Noteworthy efforts have already been made by the academic and research organizations to build secure computing infrastructures but various challenges are stay alive in security procedure of MCC. This manuscript provides a broad analysis of confidentiality and security challenges in mobile cloud computing and also discusses how to overcome these loopholes.*

Key Words: Mobile Cloud Computing, Privacy, Security, Protective Measures

Introduction

Smartphones and tablets are becoming a significant part of our routine life. Before to acquire a depth understanding of MCC, it is necessarily required to obtain the basic knowledge of cloud computing. According to the National Institute of Standards and Technology, Cloud Computing (CC) is a model for permitting appropriate, everywhere, on-request network access to a shared pool of configurable computing resources like storage space, applications, servers & other facilities which can easily be delivered with least administration pains or service provider communication. Mobile Cloud Computing (MCC) has become a way to increase the capacities with no investing in innovative infrastructure, licensing fresh software or training the new workforce.

Cloud computing is also economical because of no need to heavily invest in IT infrastructure by the consumers. Cloud computing follows PAYG (pay as you go) model which means the consumer will pay for services as the consumer will use [1]. As soon as a particular user released the resources, these can be reused by the cloud provider which results in improved resource utilization.

Mobile computing has become an influential trend in the IT knowledge and business field. Mobile devices have limited hardware and software potentials but MCC provides large and more powerful computing capabilities, which help the mobile devices to perform the complex task that requires more computational power. Even though MCC has several benefits like reliability, scalability, extended storage and battery life, it also faces several challenges such as privacy, security, authentication, data management, heterogeneity, and data transfer. So, there is a dire need to address these issues to facilitate mobile cloud service users to easily gain the benefits of MCC.

In order to solve the inherent problems in mobile computing, the notion of computation and offloading in cloud computing is utilized. However, special care must be observed before offloading the job on a cloud server by taking into account the network environment and communication transparency to formulate offloading valuable for mobile customers. It is necessary to ensure the reliability and security of multimedia data

[*] Assistant Professor, Department of Computer Sciences and I.T, The Islamia University of Bahawalpur, Punjab, Pakistan. Email: khan.dostkhan@gmail.com

[†] Visiting Lecturer, Department of Computer Sciences and I.T, The Islamia University of Bahawalpur, Punjab, Pakistan.

[‡] Lecturer, Department of Computer Sciences and I.T, The Islamia University of Bahawalpur, Punjab, Pakistan.

transmission between media cloud and mobile customers as information can be shifted and stored in the cloud system via wireless that can be exposed from the security point of view.

This manuscript is arranged as follows: Section II explains the knowledge obtained from the literature review, problem statement define in Section III, Section IV explains the background of MCC, Section V portrays the architecture of MCC, Section VI expose the assessment criteria for data and application security framework, Section VII explain the confidentiality and security challenges facing by the MCC, Section VIII describes the protective measures for MCC and finally Section IX provides the conclusion of this research.

Literature Review

Khan et al conducted a survey to investigate the different security frameworks proposed for the MCC environment [2]. They disclosed that offloading maximizes the processing ability of mobile devices and the users disburse for utilizing the cloud services in a pay-as-you-go model. User privacy and mobile application security is the most challenges aspect of MCC. To ensure the data integrity, security of the application, proper data access, authorization authentication and data confidentiality, service providers are required to take special measures.

Alizadeh et al explained that privacy, as well as security, is the most serious concern in mobile cloud computing [3]. Due to inimitable requirements, opportunities, features, and challenges in MCC, authentication is immature in MCC. They analyzed the present authentication methods in MCC on the basis of efficiency, privacy, security, and usability and concluded that the present authentication techniques are based on traditional authentication schemes without taking into account the specification of MCC.

With the remarkable development in MCC, its security solution has become more focus research area. Authors concisely reviewed the advantages of MCC and analyze its privacy and security problems from 3 layers, such as mobile terminal, mobile network, and mobile cloud and suggest some protective measures (privacy protection, anti-malware, encryption, access control, and key management) [4].

MCC has overcome the hardware restraint of mobile devices. Noor et al presented a comprehensive survey of the present architecture of MCC by focusing on the last eight years from 2010 to 2018 [5]. They compared the MCC with conventional cloud computing and proposed a general architecture to evaluate thirty recent representatives MCC research architectures by utilizing a set of evaluation criteria. They also identified various research challenges like privacy, security, data transfer, and its management, bandwidth, heterogeneity, synchronization, and energy effectiveness that required the auxiliary analysis.

A critical analysis is made by the authors to investigate the various security frameworks projected for MCC environment and concluded that the most demanding aspects in MCC are assuring the security of applications and user privacy [6]. They further disclosed that there is dire need to address the various issues in MCC, such as data security, data integrity, network security, data confidentiality, authorization, data access, authentication, and many other aspects by the service providers in order to ensure the secure MCC environment.

Authors discussed the 3 representative cloud architectures which are planned to help the novel mobile computing models in the cloud and also described the various terrorization against the accessibility, integrity, confidentiality of MCC architectures [7]. They also described that malicious users can easily target the resources and protocols in an MC environment as compare to the conventional client-server architectures. In order to ensure the necessary security for MCC architecture, they proposed the defense mechanism.

Now everything is connected everywhere with the progress of ubiquitous computing but the vulnerabilities and intrusions are also increased due to system complexity and difficulty to manage each access challenge [8]. It has been presented as probable expertise for mobile services with the exponential enlargement of mobile applications [9]. It refers to the infrastructure where data storage, as well as processing, can be done away from mobile devices. Shariati et al concluded that cloud computing can lead to reduce cost and increase agility if it is used in an appropriate manner [10].

Problem Statement

Although, noteworthy efforts have already been made by a number of organizations and academia to construct the secure computing infrastructures, however, confidentiality and security challenges motivate the researchers to do more in this domain to maximize the trust of users as well as network providers on mobile cloud computing.

Background of Mobile Cloud Computing

Mobile Computing

It mainly based on the capability to utilize computer resources via mobile appliances and execution of tasks that have been conventionally performed by desktop computers. Generally, mobile computing is maintained by three basic perceptions, such as communication, software, and hardware.

Hardware developed mobile devices such as tablet, smartphones, etc. that can be used by the users and the applications software are designed and developed for execution of jobs in mobile environment. The mobile computing environment maintains the mobility, multiplicity of network access categories, numerous network disconnection and meager security and consistency [5].

Cloud Computing

Its elementary aim is to maximize the power and ability of IT networks by consolidating how information is processed and stored. Cloud computing enables the users to get access to applications with no need for installations and also store the personal data on the internet which also reduces the building cost of IT infrastructure or getting more resources. Cloud services are well described by the following 5 vital characteristics which as under: -

a. On-request self-services
b. Resource pooling
c. Swift elasticity
d. Wide network access
e. Calculated services
i. Cloud Service Delivery Models

According to the CISCO, the IoT is gradually mounting the potentials of the cloud [11]. The major 3 cloud service delivery models are discussed as under: -

Software as a Service (SaaS)

SaaS is a software deployment model whereby the mobile service provider licenses an application to mobile users for utilization as a service on request. SaaS allowed mobile users to utilize the application offered by the cloud service supplier through the internet and they will pay for service. A customer does not own the software just use and pay for usage. Examples of Software as Service providers are Google, Zoho, Salesforce, and Microsoft, etc.

Platform as a Service (PaaS)

PaaS offers the facilities in the shape of development gadgets, programs, architecture, IDE, and framework. By means of this service, users are able to manage the application except handling the fundamental infrastructure. It is helpful when several developers located at a different physical location are required to work together. It is more flexible and extensible as compare to SaaS. Example of PaaS supplier is Salesforce.com, Google App Engine, etc.

Infrastructure as a Service (IaaS)

It deals with the computer hardware which includes: storage, network, data center, processor, memory, and other computing resources. The mobile users can run various software including operating systems as well as applications. However, IaaS has still security concerns, which require special attention.

Cloud Deployment Models

Generally, cloud computing based on collective resources by neighboring servers or individual devices [12]. With the benefit of resource allocation, it achieves consistency. The cloud deployment model tells regarding the nature of the cloud. Following four models (Public, Private, Community, and Hybrid) are utilized to organize a cloud computing infrastructure: -

Public Cloud

This deployment model has a proprietary infrastructure, which may be kept inside the domestic data hub of an association at the back of a firewall [13]. A private cloud is run and handled only for a solitary group and the group may possess or not possess the physical infrastructure.

The private cloud can be controlled by a third party or the company itself. As the infrastructure owned and controlled by a similar company, so, it is simple to find out the affiliation between the consumer and vendor and also trouble-free to detect the security flaws in the private cloud.

Private Cloud

Cloud service providers owned the cloud physical infrastructure and open access provided to the organization as well as the public. In order to preserve the confidence between cloud service providers and customers, there should be a strapping service level (SAL) harmony between them. The physical infrastructure is located off-site, which makes this model riskier, so, precautionary measures must be observed.

Community Cloud

Multiple organizations have controlled and shared this deployment model. Their interests such as mission, security requirements and policy are common. Several communities can liberally access the information in the cloud. Any organization or a third party in the society can manage the community cloud. Cost of private clouds and security risks of public cloud reduced by the community cloud.

Hybrid Cloud

It is the amalgamation of two or additional foresaid deployment models of cloud. It is more secure and well organized as it resembled the public cloud. This deployment model of cloud is situated both on-site as well as off-site places. It also allows different parties to get data over the internet.

The architecture of Mobile Cloud Computing

Mobile devices are now omnipresent in our routine life, which motivates the organizations to develop more and more applications that can easily be acquired via smartphones. But the limited resources of CPU, memory and storage capacity of smartphones enforce design constraints to mobile apps developers.

Figure 1 shows the basic architecture of MCC comprising of 3 different layers which are described as under:

Mobile User Layer

It comprises of various cloud service users who access these services by utilizing their mobile phones.

Smartphones and tablets connect to this layer using WAP, Satellite or BTS.

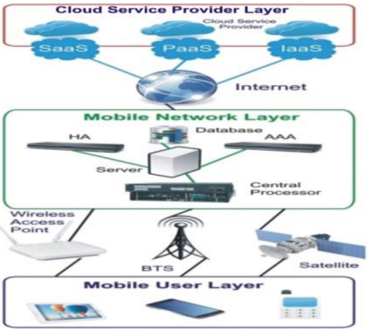

Figure 1: The architecture of Mobile Cloud Computing

Mobile Network Layer

It comprises various network operators that hold mobile consumer's demand and data is sent via Base Station (BS). Mobile consumer's requests and information are tackle by mobile network services like accounting, authorization, and authentication that are supplied by the home agent, whereas, mobile network operators assist to find out the information of the subscribers. Network operator sends the mobile consumer's request to the cloud via the internet but it could be done after booming authorization and authentication. After that, the mobile consumer is able to access the relevant services.

Cloud Service Provider Layer

It comprises of various cloud computing service providers that ensure all kinds of cloud computing services like SaaS, PaaS, and IaaS. These facilities are provided to the consumers on their demands.

Assessment Criteria For Data and Application Security Frameworks

Various frameworks of security are presented by the authors in their survey papers which deal with the security and privacy issues in MCC. Present security frameworks for MCC are divided into two groups. In the mobile computing environment, computational requirements, assumptions, and scalability played a vital role in the successful utilization of security frameworks. Mobile consumers always try to store their extra or huge files on a cloud server without revealing the classified data. It must be ensured that the security framework should provide confidentiality and security to mobile consumers.

Assessment Criteria of Data Security Framework

Mobile users' files security deals with the data security framework. For comparing the existing security frameworks, the following assessment criteria have been selected.

Basic Hypothesis

The basic hypothesis criteria define the basic building blocks of the security framework of mobile cloud computing. Here, mathematical and cryptographic keys are the basic building blocks

Data Integrity

Mostly mobile consumers upload their data on the cloud server in order to maximize the storage capability, so, a proper mechanism should be ensured for the correctness of mobile users' data. With the assistance of integrity verification, the accuracy of the uploaded files can be confirmed.

Data Scalability

With the passage of time, the number of users is increasing, so, the need for the scalability also maximizes, so the security framework must keep the quality of scalability. The scalability of the framework is regarded as reasonable if the proposed framework of security only depends on a number of the centralized servers which supervised by a 3rd party to ensure better protection characteristics.

Data Accessibility

Data accessibility is assumed to be automated if consumers allocate the encrypted files which are resided on cloud servers amongst the other users and only the certified consumers can obtain and decrypt the files mechanically with no physical intervention of the file's holder.

Data Authenticity

The security framework must ensure a proper method to confirm the original creator of the file so that during sharing multiple users' data may not be mixed up.

Assessment Criteria of Application Security Framework

The security of the mobile appliance is ensured by the application protection framework that used the cloud recourses to ensure the best services to mobile customers. Some assessment criteria of application security framework as discussed as under:

Mobile Application Type

This assessment criterion is utilized to find out the mobile application kind whose safety uniqueness is enclosed in the mobile cloud computing surroundings.

Security Features

This parameter finds out the enclosed safety characteristics such as location and identity privacy, authentication, safe information access management and risk management of mobile application models in the mobile cloud computing environment.

Applications Scalability

The proposed security framework must be scalable especially when the number of users increases then performance should not be decreased. The scalability of the framework is considered good if the planned security framework only depends on a number of the centralized servers supervised by a 3rd party to ensure better safety characteristics otherwise, there will be poor scalability of applications.

Confidentiality and Security Challenges Facing by MObile Cloud Computing

Challenges for Mobile Users

The mobile user layer has the following uniqueness: support for third-party software, internet access at any time and anywhere and the open operating systems. Some challenges are described below: -

Malware

Malicious users always find soft targets to fulfill their nefarious designs. For example, attackers can upload a picture, which holds malware and if the image is not properly deleted by the users, hackers can easily get its access, so, the secret information of the users can be exposed. A number of security providers have already developed a variety of antivirus for mobile devices but with the increase of malevolent attacks, anti-malware protection could be failed. Similarly, malware can access users' secret information in various ways like 4G Network, MMS attachment, Bluetooth or USB interface.

Software Vulnerabilities

Application Software

Mobile device users managed their smartphones through mobile device executive software that handles the file in the mobile device via content management between a computer and mobile phone. For this process, a file transfer protocol is generally applied. The username and password are shifted over the network and stored in the configuration file in plain text which can be caused any illegal access to the users' smartphones by utilizing file transfer protocol from the computer in the same network and finally the users' private data could be leaked and any malicious user can be utilized this data for illegal motives.

Operating System

The operating system played a key role in security and privacy as OS is responsible for the management and control of the software as well as hardware. Sometimes, users installed complex software in their mobile phones which carries serious bugs and these bugs could be utilized by the attackers to destroy the mobile phone.

Challenges for Mobile Network

Conventionally, the mobile network enlarges the network node and the entrance mode of users. As the network node is enlarged to various mobile devices like tablet PC and smartphones, mobile devices can get admission to the network from various ways like Wi-Fi and Bluetooth which can bring security threats. User's personal information or data can be leaked and some malicious users utilized this data for illegal motives which is very harmful. So, in the situation of malevolent spoofing and sniffing of a virtual network, the cryptography keys become exposed. Furthermore, contact among the clients and the cloud services suppliers is made frequently via various interfaces, which is also a security risk.

Challenges for Cloud Service Providers

Platform Reliability

Due to the high absorption of information resources of customers, the mobile cloud platform is vulnerable. Malicious users always try to access this valuable information. Cloud computing staff or malicious attackers can be harmful in the cloud computing environment. Sometimes, users not select the backup and recovery services and faced a lot of trouble in shape of loss of their precious data. Therefore, the cloud service suppliers must interrogate the present security measures; otherwise, users may not depend much on them.

Data Integrity and Privacy

Data integrity and secrecy are the key elements of any computing environment, therefore, cloud computing providers always try to ensure these characteristics but up to some extent, therefore, necessary security measures are required to be taken forthwith. With the passage of time, numbers of mobile users are increasing, so, the security must be strengthened in MCC, in order to ensure data integrity and confidentiality. Cryptography approach in MCC is not well versed, which also decreased the data integrity. Data security is another issue of mobile cloud computing as encryption algorithms having bulky keys are not run on mobile devices due to least processing power of these appliances.

Data Recovery Vulnerability

Resources assigned to some particular customer may be allocated to some other customer (maybe a malicious user) in the later stage, who can use the recovery tools and recovered the data of previous users which is a great risk. Data recovery vulnerability can cause a serious security breach, so, an extra vigilance of cloud service providers is required in mobile cloud computing.

Energy Efficiency Challenge

It is the most significant problem in MCC due to the restraint of mobile hardware. CPU, Bluetooth, Screen, Wireless Network Interface card and GPS consume more power in smartphones. Wi-Fi and 4G networks consume more power and there are extra concealed costs for mobile consumers which should be influenced by the acceptance of MCC. Hence, there is a dire requirement for well-organized techniques in order to improve the energy optimization that will be helpful for mobile consumers and also increase the interest in MCC.

Identity Management and Access Control

Cloud deals with different users having different authentication and authorization framework, so, it is much more difficult to keep the record of customers' identity, so that, only the authorized users can access the resources. Cloud required a strict access control mechanism to restrict unauthorized access to malicious users. Many issues can arise in case of week identity management and access control like cross-domain validation, chances of inadequate logging and monitoring, XML wrapping attacks, DoS by account keep off, etc.

Protective Measures for Mobile Cloud Computing

In fact, MCC facing a lot of challenges but it also provides greater efficiency and flexibility to mobile users. Some protective measures for MCC are discussed as follow:-

Mobile User Security

Mobile user's security can be ensured by utilizing anti-malware, removing software vulnerabilities and regulating user's behavior.

Anti-Malware

There are two things to do, first is to find out and eliminate the malware. It means, when malware found, legal software must be assigned by the cloud service suppliers and be run to eliminate the malware forthwith. CloudAV is a good instance of anti-malware which a model for malware discovery on mobile workstations [4]. It provides various significant benefits like removing the impact of antivirus vulnerabilities, helpful in detecting the past infected host, superior detection of malevolent software, enhanced deploy management and also enhanced the forensic capacities.

Second is the prevention of the malware attack. It has been observed that the second option is more suitable as compared to first, so mobile users should be more careful. Prevention strategies are discussed in detail as under:

Remove Software Vulnerabilities

Mobile users should pay special attention to updating information on their mobile operating system (OS), in time download and set up the upcoming patches from the growing organization of the OS. During downloading third-party software, mobile users must observe special care to avoid any software vulnerability. Furthermore, technical measures like checking of legitimacy and integrity of the software should be observed before its installations.

Regulating Users' Behaviour

Due to the lack of security consciousness, mostly malware is downloaded during software installation as users do not care about it. So proper guidance of people about malware can prevent them from any malicious attack. For example, people mostly click on unexplained links without reading its descriptions which results in leakage of users' classified information. So the users must be aware of such attacks and they should avoid installation of new unauthorized software. No need to keep on the Wi-Fi and Bluetooth unnecessarily.

Mobile Network Security

Protocols defined for communication have already proved in danger to various attacks. For example, the SOAP (Simple Object Access Protocol) message can be influenced to target cloud platform services and breach data protection. Therefore, strong encryption mechanisms can ensure data security as only encrypted data is becomes safer throughout the broadcasting over the network. Another aspect of mobile network security is the security protocol that can reduce the chance of malicious attacks.

Mobile Cloud Security

Security to Ensure Platform Reliability

The availability, as well as reliability of MCC, is of utmost importance for both the mobile users as well as cloud service suppliers. Cloud service suppliers should strengthen the present security measures such as authentication and encryption against different attacks like Denial of Service attacks and information pilfering. They also provide the complete backup and recovery service to mobile users as and when a malicious attack took place. All these protective measures should be observed by the cloud service suppliers to progress the eminence of service as well as maximize the assurance of the users on MCC.

Data Encryption and Key Management

The classified data of customers required encryption expertise so that the data can safely transmit from storage. The data must be stored at the cloud in cipher-text to prevent sensitive information from leakage. Although, cipher-text provides complete security, however, it also reduces the data utilization rate, so there must be a focus on efficiently processing and evaluating the cipher-text. As per the Cloud Security Alliance recommendations (CSA), the following precautionary steps must be observed for data storage and key administration [14]: -

- Either the organization or users themselves should be performed the Key management and it may also be ensured by a trusted cryptographic service.
- Off-the-shelf-technology should be used.
- Proprietary algorithms may not be used, only standard algorithms should be used for better security measures.

Identity Management and Access Control

According to CSA recommendations, the following precautionary measures must be observed for Identity management and access control [14]:-

- The source of an attribute should be closed to the main source.
- Attributes must also be authenticated at the main source.
- For a secure relationship and transactions, bi-directional trust must be ensured.

To offer the right of entry in the cloud setting, Attribute-Based Encryption is used which cryptographically apply the access control policies. Authors have introduced individuality management and function-based control scheme called Role Base Multi-tenancy Access Control (RB-MTAC) [15]. In this scheme, the user sets the password and gets registered himself with cloud and obtains a unique identity.

Data Privacy

Many countries have already developed safety rules to protect data privacy. To fulfill the requirement of cloud development and deployment, confidentiality requirements should be defined properly. The probabilistic PK encryption method and keyword probing algorithm can be used to preserves the privacy of mobile devices [16]. To accumulate data on clouds, authors proposed a lightweight cryptographic technique for mobile devices [17].

Conclusion

Where mobile cloud computing provides premium services to mobile users through the effective utilization of shared resources there it also faces various confidentiality and security challenges that obstruct the fast rate acceptance of mobile cloud computing. This manuscript articulates the background of MCC, its architecture, assessment criteria of the security frameworks, confidentiality and security challenges and its countermeasures that will be helpful for cloud service providers as well as researchers for future exploration of this domain. Cybercrime is becoming more sophisticated as malicious users are being followed by the new trends & tactics to fulfill their wicked desires, therefore, more robust methods are required to be adopted to handle the tough requirements of mobile cloud computing.

References

Ali, M., Khan, S.U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357-383.

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S. & Sakurai, K. (2016). Authentication in Mobile Cloud Computing: A Survey, *Journal of Network and Computer Applications*, 61, 59-80.

Bahrami, M. & Singhal, M. (2015). A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, In 3rd IEEE International Conference on Mobile Cloud Computing, Services and Engineering, pp. 189-198.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire M. M., & Indcio, P. R. M. (2014). Security issues in cloud computing. *International Journal of Information Security*, 13, 113-170.

Gu, Q. & Guirguis, M. (2013). Secure Mobile Cloud Computing and Security Issues, *High Performance Cloud Auditing and Applications*, 65-90.

Khan, A. N. , Kiah, M. L. M., Khan, S. U., & Madani, S. A.(2013). Towards Secure Mobile Cloud Computing: A Survey, *Future Generation Computer Systems*, 29 (5), 1278-1299.

Kulkarni, P.& Khanai, R. (2015). Addressing Mobile Cloud Computing Security Issues: A Survey, In IEEE International Conference on Communication and Signal Processing (ICCSP), pp. 1463-1467.

Kulkarni, P., Khanai, R.& Bindagi, G. (2016). Security Framework for Mobile Cloud Computing: A Survey, In IEEE International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT), pp. 2507-2511.

Noor, T. H., Zeadally, S., Alfazi, A., & Sheng, Q. Z. (2018). Mobile Cloud Computing: Challenges and Future Research Directions, *Journal of Network and Computer Applications*, 115(1), 70-85.

Pasupuleti, S. K., Ramalingam, S., & Buyya, R. (2016). An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. *Journal of Network and Computer Applications*, 64, 12-22.

Sahmim, S.& Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review. Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 21st International Conference, pp.1516-1522.

Shariati, S. M., Abouzarjomehri & Ahmadzadegan, M. H. (2016). Challenges and Security Issues in Cloud Computing from two perspective: Data Security and Privacy Protection, In IEEE International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 1078-1082.

Savu, L. (2011). Cloud Computing: Deployment models, delivery models, risks and research challenges, In IEEE International Conference on computer and management, pp. 1-4.

Singh, ,S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: issues, threats and solutions, *Journal of Network and Computer Applications*, 75, 200-222.

Suo, H., Liu, Z., Wan, J. & Zhou, K. (20130. Security and Privacy in Mobile Cloud Computing, In IEEE 9th International Wireless Communication and Mobile Computing Conference (IWCMC), pp. 665-659.

Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34, 1-11.

Yang, S. J., Lai, P. C., & Lin, J. (2013). Design role-based-multi-tenancy access control scheme for cloud services, In IEEE International Symposium on Biometrics and security technologies, pp. 273-279