

Security and privacy challenges in mobile cloud computing: Survey and way ahead


Muhammad Baqer Mollah

Cite this paper

Downloaded from [Academia.edu](#) 

[Get the citation in MLA, APA, or Chicago styles](#)

Related papers

[Download a PDF Pack](#) of the best related papers 



[Data Security in Mobile Cloud Computing: A State of the Art Review](#)

Rida Qayyum

[Key Exchange Techniques Based on Secured Energy Efficiency in Mobile Cloud Computing](#)

Karthik Bala

[Access Control for Fog/Cloud Enabled IoTs](#)

Journal of Computer Science IJCSIS



Review

Security and privacy challenges in mobile cloud computing: Survey and way ahead

Muhammad Baqer Mollah^{a,*}, Md. Abul Kalam Azad^a, Athanasios Vasilakos^b^a Department of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh^b Department of Computer Science, Electrical and Space Engineering at the Luleå University of Technology, Sweden

ARTICLE INFO

Keywords:

Mobile computing
Cloud computing
Computational offloading
Virtualization
Security and privacy

ABSTRACT

The rapid growth of mobile computing is seriously challenged by the resource constrained mobile devices. However, the growth of mobile computing can be enhanced by integrating mobile computing into cloud computing, and hence a new paradigm of computing called mobile cloud computing emerges. In here, the data is stored in cloud infrastructure and the actual execution is shifted to cloud environment so that a mobile user is set free from resource constrained issue of existing mobile devices. Moreover, to avail the cloud services, the communications between mobile devices and clouds are held through wireless medium. Thus, some new classes of security and privacy challenges are introduced. The purpose of this survey is to present the main security and privacy challenges in this field which have grown much interest among the academia and research community. Although, there are many challenges, corresponding security solutions have been proposed and identified in literature by many researchers to counter the challenges. We also present these recent works in short. Furthermore, we compare these works based on different security and privacy requirements, and finally present open issues.

1. Introduction

The mobile computing is the fast-growing business solution in the field of Information and Communications Technology (ICT). The number of mobile users is escalating due to constantly improving user friendly hardware and software of mobile devices (Chung et al., 2014; Ba et al., 2013). At present, the mobile devices such as smartphones and tablets are not only used as a traditional mobile phone but also used as emailing, chatting, internet browsing, running a wide range of applications, file sharing, reading or editing documents, entertaining etc. From the market analysis, it was predicted that the number of usage of tablets and smartphones would be 640 million and 1.5 billion, respectively within 2015 globally (Online, 2016). However, the mobile computing alone fails to meet the full satisfaction of the large number of users and their computational requirements.

The mobile cloud computing (MCC) is introduced as services of cloud computing, which is offered in either mobile phone environment or mobile embedded system environment. Mobile computing is integrating with cloud computing because of the essential characteristics of cloud model such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. Moreover, the cloud computing is being popular to the mobile users

as it can provide cloud like services (Mollah et al., 2012; Buyya et al., 2009). According to the ABI research report about the increasing popularity of MCC (Online, 2016), it was forecasted that within 2015, more than 240 million of mobile customers will use cloud services with an earning revenue of \$5.2 billion. However, to avail cloud services, mobile devices are depended on wireless communication technologies (Fernando et al., 2013; Sharma et al., 2013; Sharma et al., 2013). The mobile computing is used to show, process, transport and share the applications and resources, whereas wireless communication is used so that the mobile users can utilize the network resources, services and support the communication between mobile devices and clouds. Now a days, there are several emerging applications of cloud computing for mobile users such as application processing (Ahmed et al., 2015; Meilander et al., 2014; Mao et al., 2017), cloud storage (Choo, 2014; Teing et al., 2016; Ab Rahman et al., 2016), data sharing (Chen et al., 2015), cloud mobile media (Wen et al., 2014; Gao et al., 2015), cloud based next generation cellular network (Cai et al., 2014; Yin et al., 2015), mobile commerce system (Yang et al., 2010), education and learning (Ferzli and Khalife, 2011), mobile social networks (Chard et al., 2010; Nan et al., 2014), gaming (Meilander et al., 2014; Cai et al., 2015), human-centric mobile cloud (Chen et al., 2015a, 2015b), cloud assisted Internet of Things (Shon et al., 2014; Psannis et al., 2014;

* Corresponding author.

E-mail addresses: m.m.baqer@ieee.org (M.B. Mollah), makazad@juniv.edu (Md. A.K. Azad), athanasios.vasilakos@ltu.se (A. Vasilakos).

Cahyani et al., 2016) etc. However, as there is tremendous advancement in the field of widespread wireless communication technologies such as Wi-Fi, fourth generation/long term evolution, advanced and future 5G millimeter wave wireless communications (Rappaport et al., 2013; Wu et al., 2015; Hossain and Hasan, 2015), the mobile users can use the cloud services in easier way than past.

In (Zhong et al., 2012), the authors show that at least six following features are essential for MCC such as breaking through hardware limitations, having suitable data access, intelligent load balancing, efficient task processing, cost effective on demand service and removing the regional boundary. Although there are several advantageous features, it has some issues and challenges (Alizadeh and Hassan, 2013; Liu et al., 2013; Amin et al., 2013), which creates some obstacles for its rapid advancement. These issues and challenges, briefly described in Section 2, are limited resources of mobile devices, stability, availability, costs of network access, scarcity of channel bandwidth, heterogeneity, process offloading, mobility management, context-processing, cloud policies for mobile users, elasticity, application services issues, energy efficiency, ensuring Quality of Service (QoS), security, trust, privacy challenges etc. Among these, security and privacy are becoming more challenging issues than others due to several reasons like insecure open air transmission medium, resource-constrained mobile devices, distributed cloud storage and processing, and heterogeneous environments.

This survey paper presents in details the security and privacy challenges that arise due to the integration of mobile computing and cloud computing. The challenges that are focused in this paper are depicted on Fig. 1. We then discuss on some recent solutions and countermeasures techniques. However, some of these security and privacy challenges are yet to be solved and under research activity. In Table 1, we try to summarize our contribution and draw a comparison with other contemporary works. At the end of this paper, a discussion on the open issues and future research directions is presented.

The rest of this paper is organized as follows: Section 2 presents the background literature of this survey; Section 3 shows the security and privacy requirements for MCC; Sections 4 and 6 deal with the security and privacy challenges of MCC respectively; Sections 5 and 6 analyze the available approaches regarding security and privacy respectively; Section 7 discusses open issues; and finally, section VIII concludes this paper.

2. Background

2.1. Mobile cloud definitions

The MCC Forum introduces the MCC (Online, 2016) as in MCC there is an infrastructure named cloud outside of the mobile devices where both the data storage and processing take place, and cloud based applications shift the computing power and data storage into the cloud, and it is not only for Smartphone users but also a wide range of mobile users. Whereas, the authors in (Sanaei et al., 2012) say in their article, the MCC is a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage and mobility, and serves a multitude of mobile devices anywhere anytime through the Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle. In summary, we can say, MCC is a combination of mobile computing, cloud computing, and wireless technology where the mobile users utilize different cloud based services as like as personal computer users.

2.2. Partitioning and offloading

Executing of mobile applications are computational-intensive, and thus, a large amount of energy is consumed by mobile devices. The computational offloading technique is introduced to overcome this kind

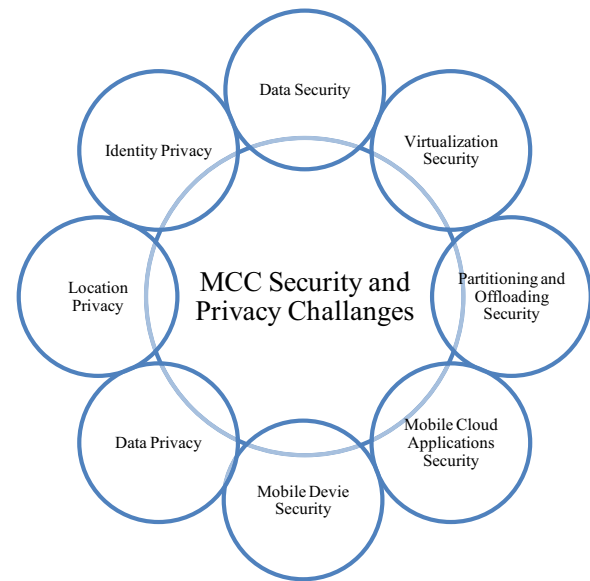


Fig. 1. Main security and privacy challenges in MCC.

of challenge. The computational intensive applications and tasks of mobile devices are offloaded to the cloud for execution, and mobile devices receive the results afterwards (Ellouze et al., 2015; Flores et al., 2015; Chen et al., 2016) and (Chen et al., 2015c). There are three steps of computational offloading process such as partitioning, migration and execution. Fig. 2 represents the offloading process from mobile device to cloud. Although the execution and processing are transferred from mobile devices to clouds, the mobile devices can make decision how to execute and how much computation needs to be offloaded to cloud according to its resources.

2.3. Mobile cloud applications

With the rapid increasing of mobile devices, various kinds of applications for these devices are developing by the developers and many of these offer cloud based services with rich user experience (Bahrami, 2015). By these applications, the mobile users can get cloud based rich experience and services even from limited resourced mobile devices. These applications need to scale up or down instantly to fulfill mobile user demands as well as mobile device capability. To offload a mobile application to cloud, the application requires to be divided into components according to its needs. The components of an application which needs local mobile resources like different sensors do not need to offload to cloud. But the components those are highly resource intensive need to offload to the cloud for execution. Therefore, these applications can be divided into three types such as client based, client-cloud based and cloud based models. In client based model, the major execution of an application is held on mobile device. But in client-cloud based model, an application is partitioned into components and these components are executed by mobile device as well as remote cloud. Whereas, in cloud based model, the cloud is part and parcel of an application where the application runs, processes, and stores.

2.4. Mobile cloud architectures

Three kinds of MCC architectures are available. These are mobile client-server, ad hoc and mobile edge-cloud architectures. The mobile client-server architecture is like as traditional client-server based cloud architecture where the mobile device and cloud are working as like as client computer and cloud server respectively. Like client computer, the mobile device is working as a user interface, and it makes request to clouds to execute and manage the computational intensive applications. Two client-server architectures are proposed in (Chun and

Table 1

Contribution of paper with respect to previously published survey works.

	(Khan et al., 2013a)	(Raj et al., 2012)	(Ali et al., 2015a)	(Suo et al., 2013)	(Alizadeh et al., 2016)	(Tep et al., 2015)	(Osanaie et al., 2016)	(Azfar et al., 2016)	(Iqbal et al., 2016)	(Juliadotter and Choo, 2015)	Our Work
MCC Overview	Yes	No	No	Yes	No	No	No	No	No	No	Yes
Security	Yes	Yes	Yes	Yes	Authentication only	Yes	DDoS Only	Yes	Yes	Yes	Yes
Privacy	No	No	Yes	Yes	No	No		Yes	No	Yes	Yes
Current Solutions	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Related Works	Yes	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Open Issues	No	No	Yes	No	No	No	Yes	Yes	No	No	Yes

(Maniatis, 2009; Giurgiu et al., 2009). Although the mobile client-server architecture can support to mobile users, it has some limitations like latency due to round trip delay, jitter and bulk data transfer within the wireless network. It also needs infrastructure and wireless access to provide services. And it may be abnormal to access to the cloud service during emergencies or natural disaster, and also where the wireless access is rare and costly. Moreover, some cloud services need the mobile devices to be aware of context of other mobile devices. In such cases, the ad hoc architecture is a solution. Here, the mobile devices form themselves an ad hoc network by using modern wireless technologies to provide cloud services each other. Two ad hoc architectures are proposed in (Huerta-Canepa and Lee, 2010; Mohammad et al., 2015). At present, the mobile applications are offloaded the computational processing task from mobile device to cloud. But latency intensive services face end-to-end communications delay, bandwidth problems and costly data services. In the mobile edge-cloud architectures, the computational tasks are processed in both cloud and nearby mobile devices or local cloud server. Hence, it can reduce the latencies between the mobile devices and clouds, network bandwidths etc. Cloudlets (Satyanarayanan et al., 2009), fog computing (Luan et al., 2015; Vaquero and Roderio-Merino, 2014), micro clouds (Wang et al., 2013) etc. are the examples of such architecture.

2.5. Mobile cloud service models

MCC has following service models to provide cloud services to mobile users.

2.5.1. Mobile Network as a Service (MNaaS)

In this service model, the service providers offer a network infrastructure so that the users can create their own networks, control the traffics, and connect to the servers. Example: OpenStack Networking Service (www.openstack.org).

2.5.2. Mobile Cloud Infrastructure as a Service (MIaaS)

In this service model, the service providers offer cloud infrastructure and storage to mobile users. Examples: iCloud (www.apple.com/icloud/) and Google drive for mobile users (www.google.com/mobile/drive/).

2.5.3. Mobile Data as a Service (MDaaS)

In this service model, the service providers supply database related services in order that mobile users can do their data management, transaction and other data related operations. Example: Oracle's mobile cloud data as a service (www.oracle.com/cloud/daas.html) and CloudDB (Lei et al., 2015).

2.5.4. Mobile App as a Service (MAppaaS)

In this service model, the users can use, access and execute cloud based mobile applications through wireless network in anywhere and anytime. Example: Applications in Google Play Store (www.play.google.com/store/apps).

2.5.5. Mobile Multimedia as a Service (MMaaS)

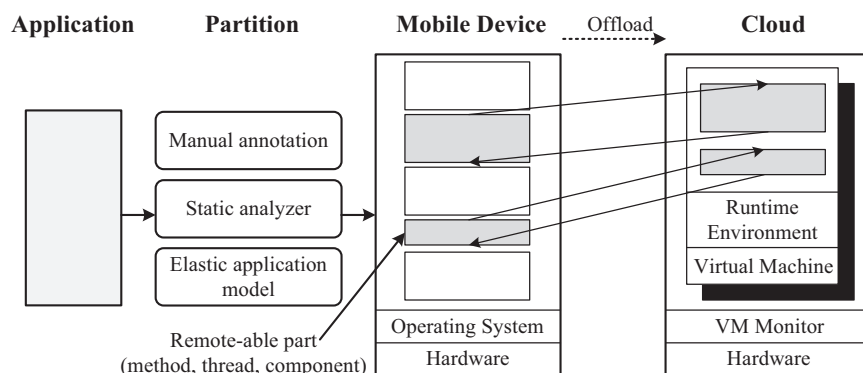
In this service model, the users can run and manage the multimedia services such as playing movies or games through the wireless network in rich hardware equipment. Authors in (Zhu et al., 2011) present a MMaaS service model.

2.5.6. Mobile Community as a Service (MCaaS)

In this service model, a group of mobile users can build and manage a mobile social network or community where the users can get provided social network or community services. An example of this kind of service model is presented in (Kovachev et al., 2010).

2.6. Challenges

Although MCC has several advantages for both mobile users and cloud service providers, it faces several challenges which make it more

**Fig. 2.** The computational offloading process from mobile device to cloud.

complicated than conventional cloud computing. In the following, we discuss the challenges faced by MCC.

- 11) *Limited Resources of Mobile Devices*: Although there have been improvement in various aspects of the mobile devices like computational processing power, storage capacity and battery power, there are still some limitations in comparison with a personal computer. As a consequence, it is inconvenient to run resource hungry applications on mobile devices.
- 12) *Heterogeneity*: In MCC, maximum of communications take place within heterogeneous wireless medium which generates more challenging environment than conventional cloud computing. This may affect in managing the wireless communications, the quality of communications, application response time, delivering the services, mobility of mobile devices, and security. Moreover, different infrastructures, platforms and application services cause heterogeneous environment resulting in interoperability and portability challenges in MCC.
- 13) *Elasticity*: Like cloud computing services, the MCC services need to have elasticity and scalability. If there are more demands than available resources, the service providers need to tackle this situation. The resource unavailability and interruptions of services result in problem for cloud services to privileged users.
- 14) *Application Services Issues*: Because of having limited resources and enormous energy consumptions, some of data and computational intensive applications cannot be deployed in mobile devices. Consequently, to utilize the cloud computing services on mobile devices, the major computational processing task needs to be processed by cloud, and a small amount of computational processing is done on mobile devices. In such case, the mobile users face delay during processing and service availing.
- 15) *Security, Privacy and Trust Challenges*: The security, privacy and trust challenges arising in MCC environment become more volatile with respect to traditional cloud computing. Moreover, it is inconvenient to run computational-intensive anti-malware applications in mobile devices as like as personal computers due to lack of computational processing capability to execute complex algorithms.

3. Security and privacy requirements of MCC

The general security requirements for MCC can be derived from the security requirements defined by ITU (Online, 2016) and US National Security Agency (Online, 2016), which are summarized in the following.

- 11) *Confidentiality*: The confidentiality is fundamental requirement that refers to keep mobile users' data secret in the cloud. Here, the confidentiality is a big hindrance for mobile users to avail the cloud services. As the data is transmitted and received within public networks, and stored or processed in public cloud servers to avail the cloud services, there is possibility to reveal the data to unauthorized parties.
- 12) *Integrity*: In MCC, the data storage and processing are resided on the service provider's end. Here, the integrity needs to ensure the accuracy and consistency of users' data. In other words, the integrity prevents undetected modification of the data by any unauthorized users or systems. The violation of integrity affects the mobile users in their business, economic and other losses.
- 13) *Availability*: For MCC, the availability ensures that all cloud services must be available always at any places as per mobile users' requirements. Ensuring availability includes preventing different kinds of availability attacks which make delay, alter or interrupt the availability of services.
- 14) *Authentication and Access Control*: The authentication is the process or act of determining the identity of a user, user's data or

application. After successful authentication process, it is needed to determine what resources are permitted to access and what kind of actions can perform such as view, run, modify or delete. This is called access control.

- 15) *Privacy Requirements for MCC*: The security objectives such as confidentiality, integrity and authentication persuade the privacy and these objectives preserve the privacy directly or indirectly of the cloud service users in mobile devices.

4. Security and privacy challenges within MCC

The MCC utilizes many traditional as well as recent technologies such as partitioning, offloading, virtualization, outsourced storage, mobile-cloud based application etc., and it adopts several new security challenges along with traditional challenges. In this section, we present the list of potential security and privacy challenges within MCC. The challenges are discussed as following categories.

4.1. Data security challenges

The major data security challenge is introduced as the consequence of mobile users' data is stored and processed at clouds that are located at service providers' ends. The data related challenges include data loss, data breach, data recovery, data locality and data privacy. The data loss and data breach break two security requirements such as integrity and confidentiality. Here, the data loss means the users' data is in error condition that damaged or skipped by any physical means during processing, transmitting or storage. In data breach situation, users' data is stolen, copied or used by any other unauthorized users. These two can be occurred by malicious insider or from outside through malicious applications. The data recovery problem is another concern. This is a process of recovering the data from damaged, failed, corrupted or lost the mobile users' data or from physical storage device. However, in cloud service models, as the users' data is stored in the service providers' premises, the users need to know where their data is located or stored, and therefore, the data locality is also a challenge. The users' data also need to store separately from others. If one users' data mix, combine or confound with other users' data, it will be much more vulnerable. Once the data is outsourced to cloud servers to extend the storage capacity, mobile users lose the physical control of their data simultaneously. Thus, the correctness of the data becomes one of the concerns for mobile users in cloud storage scenario. Although the cloud infrastructures are much more reliable and powerful than mobile devices, they are still facing a multitude of threats from internal and external for data integrity.

4.2. Partitioning and offloading security challenges

During offloading process, there requires to access to cloud through wireless networks. Since the mobile users do not have any access and control over their offloading processes, hence, there is a risk of unauthorized access to offloaded content. And due to the offloading content executions are done within the cloud or edge servers instead of mobile device, there is also possibility to violate the integrity and confidentiality of offloaded contents. The integrity challenge arises due to after execution of offloaded content, if the result is not correct or altered, the mobile devices can not verify easily the correctness of the results. However, other challenges include availability attack and malicious content threats. The jamming attack between data/application and mobile device during partitioning, and between mobile device and cloud during offloading can affect the availability of cloud services. And the presence of malicious content in-between the partitioning and offloading stage can impact on the users' data confidentiality as well violate the privacy of mobile users.

4.3. Virtualization security challenges

In MCC, the cloud service providers offer cloud services using virtualization techniques to the mobile users. In cloud end, an image of virtual machine (VM) of the mobile device is pre-installed and the tasks of the mobile device are offloaded to the VM for processing. This VM is also called thin VM or phone clone. The main function of virtualization is to provide several VMs running in a same physical machine or mobile devices and the VMs are isolated from each other. An additional layer called hypervisor or VM Monitor or Manager (VMM) is software that allows creating, running and controlling VMs and its other virtual subsystems. However, virtualization techniques when applied to MCC, generates several security challenges (Sgandurra and Lupu, 2016) such as security challenges within the VMs, unauthorized access, VM to VM attack, communication security within the virtualized environment, security challenges within the Hypervisors and confidentiality of data.

4.4. Mobile cloud applications security challenges

The cloud based mobile application level attacks can affect the integrity and confidentiality of both the data and applications by different strategies, for example, integrating malwares (Pokharel et al., 2017; Prokhorenko et al., 2016; Peng et al., 2016; Quick and Choo, 2016). The malwares such as virus, worm, trojan, rootkit, botnet (Arabo and Pranggono, 2013) are unfavorable, contrary, intrusive, bothering applications or programmed codes. The targets of these malwares are to run with intentions at mobile devices or attach with applications without users' compliances. As a consequence, the functionalities of mobile applications can be changed. Generally, an attacker identifies a target application, insert malicious codes into the targeted application and finally, republish it.

4.5. Mobile devices security challenges

There are some physical threats to mobile devices. It is possible to loss, leakage, access or unintentionally disclose of the data or applications to unauthorized users, if the mobile devices are misplaced, lost or theft (Milligan and Hutcheson, 2008). Although there are password or pattern based locked features; many mobile users do not use these features. And the identity module card inside the mobile device also can be taken aside from device and accessed by unauthorized persons. Moreover, most of mobile devices are lack of security mechanism against threats. The attackers can attack by utilizing different availability attack techniques such as by sending high malicious traffic stream, huge messages to targeting mobile devices to make unused or reducing the capability. Lei Liu et al. (Liu et al., 2009) study and identify some security mechanisms and critical vulnerabilities of security models for smart mobile devices. In addition, the authors show how a distributed denial of service attack is launched by utilizing the vulnerabilities. However, the battery power exhaustion attack is another kind of availability attack where after attacking, the mobile devices start to discharge its battery power rapidly. This attack is unique for mobile device as it is performed by utilizing vulnerabilities of wireless networks, and mobile users are unaware about this kind of attack. In (Racic et al., 2006) the authors discuss about this kind of attack. Here, they show by this attack, the power of mobile device's battery run out up to 22 times faster than its normal condition and finally, the mobile device is useless within a small amount of time.

Due to increasing the popularity of mobile devices as well as mobile applications, the malware writers or attackers pay their attentions here. Consequently, the malwares are serious security concerns for mobile users' privacy, applications and data. Moreover, the functionalities of present mobile platforms are quite close to personal computers but with extra features and these platforms for mobile devices support many applications. Hence, to ensure confidentiality and integrity of these applications, there need to secure the mobile platforms also. And

these mobile platforms are not free from malware threats. Commonly, by malware, attackers may achieve root permissions on mobile devices and can control the mobile device, and after that it may directly affect mobile platforms' computational integrity along with applications.

There are three kinds of storage available in mobile devices such as on device storage, plugged in storage and identity module storage. Generally, users' personal data, applications and others are stored in these storages. But if a mobile user avail cloud services, its data and applications are copied in the cloud storages. So, if the mobile device is stolen or lost, then it becomes an important point such as the attackers can get access to the mobile devices and access to the cloud as well.

4.6. Privacy challenges

Privacy is one of the major challenges as the mobile users' confidential data or applications are processed and shifted from mobile devices to the heterogeneous distributed cloud servers while availing different cloud services. These servers are located at different places that are owned and maintained by the service providers only. Here, the users can not physically be worth the storage of their data and thus, data privacy and protection related challenges are in the hands of service providers, and the users are not accountable for privacy lost.

Cloud storage and processing in multiple locations raise privacy problems. The cloud servers of service providers are located at different regions and countries. For example, Google's cloud servers are located almost around the world such as seven locations in Americas, two locations in Asia and three locations in Europe (Online, 2016), (Online, 2016). Moreover, it is important to users to get cloud hosting location's information as the law differs from one country to another.

Several mobile applications are available which may be unsafe due to having hideous functions, collecting unconsciously users' personal information such as hobbies, locations, and may spread illegally. The unwanted advertising e-mails or junk emails can violate the users' privacy.

The context awareness, enabled by the sensors on mobile devices, is one of the main features of mobile applications that differs from personal computers. The context provides information to service providers by giving users' context and hence, the service providers can provide services with respect to the requirements of users. These location-aware applications and services specifically raise privacy concerns for mobile devices. These can either be user invoked or service provider invoked, and need the user location's knowledge to deliver the location based services. Moreover, many applications need and collect users' location information and it can also use in advertisement purposes to the clients directly based on their locations. Therefore, the location based services raise privacy challenges as there need collect, store, process the information of users.

5. Current security solutions and related works

This section presents current security solutions and related works of aforesaid security and privacy challenges that have been proposed recently in different journals and conference proceedings. Moreover, a summary of related works is presented as tabular format in Tables 2–6. In these tables, we highlight the security features as well as the scalability of the presented works.

5.1. Data security solutions

To ensure data security in MCC, the authors propose a framework in (Alqahtani and Kouadri-Mostefaou, 2014) which is based on distributed multi-cloud storage, data encryption and data compression techniques. In this framework, firstly, the data is divided into different segments at mobile device end according to user preference, and then, the segments are encrypted and compressed. Finally, it keeps storage on distributed multi-cloud. However, user can store one segment on its

Table 2

Comparison of presented approaches dealing with data security solutions.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
(Alqahtani and Kouadri-Mostefaou, 2014; Abdalla and Pathan, 2014)	Multi-clouds for secure storage of data	Data Confidentiality	Distributed multi-cloud storage, cryptography and data compression	High
(Wang et al., 2014)	Secure data storage and sharing in mobile media cloud	Authentication and Data Confidentiality	Scalable watermarking and Reed-Solomon coding	High
(Louk and Lim, 2015; Baharon et al., 2015)	Data storage security	Data Confidentiality	Homomorphic encryption	Low
(Khan et al., 2014)	BSS, Block based sharing scheme	Data Confidentiality	Block based cryptographic system	High
(Gai et al., 2016)	Dynamic Data Encryption Strategy (D2ES)	Data Confidentiality	Selective encryption strategy under timing constraints	Moderate
(Yang et al., 2015)	Extended Proxy-Assisted Approach	Data Confidentiality	Attribute based Encryption	High
(Yu et al., 2014)	A public auditing protocol for secure data storage and sharing	Data Integrity, Identity Privacy Protection	Asymmetric group key agreement and proxy re-signature	Medium
(Sookhak et al., 2017)	Remote data auditing for secure data storage	Data Integrity	Algebraic signature and new data structure model named divide and conquer table (DCT)	High
(Yu et al., 2016)	Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy	Data Integrity	zero knowledge proof systems, proxy re-signatures and homomorphic linear authenticators	High
(Tian et al., 2015)	Dynamic hash table based public auditing	Data Integrity and Data Privacy	Two-dimensional data structure, homomorphic authentication	Moderate
(Qiu et al., 2016)	Proactive dynamic secure data scheme (P2DS)	Access Control	Attribute based access control mechanism	High
(Jin et al., 2015)	Secure and lightweight ciphertext-policy attribute based encryption (SL-CP-ABE)	Access Control	Ciphertext-policy attribute based encryption (CP-ABE) algorithm	High
(Odelu et al., 2016)	CP-ABE-CSCTSK (CP-ABE- constant size ciphertext and secret keys)	Access Control	Ciphertext-policy attribute based encryption (CP-ABE) algorithm	Medium
(Li et al., 2016)	Intercrossed Secure Big Multimedia Model (2SBM)	Access Control	Semantic-Based Access Control	High
(Li et al., 2015)	Efficient multi-keyword ranked search (EMRS)	Secure Data Searching	Relevance score, secure k-nearest neighbor technique, an efficient index and blind storage system	High
(Guo et al., 2016)	Fine-grained Database Field Search	Secure Data Searching	Attribute based encryption	Moderate
(D Liu et al., 2015)	Personalized search over encrypted data and secure updates (PSU)	Secure Data Searching	Bloom filter, k-nearest neighbor technique, modified attribute based keyword search and vector-space based search technique	High
(Zhang et al., 2016)	Attribute based data sharing in MCC	Secure Data Sharing	Ciphertext-policy attribute based encryption and symmetric encryption	High
(JK Liu et al. 2015)	Secure real time video sharing and searching in MCC	Secure Data Sharing and Searching	Advanced Encryption Standard, Searchable Symmetric Encryption, CP-ABE and Digital Signature	High
(Yang et al., 2016)	Conditional proxy re-encryption (CPRE)	Secure Data Sharing	Cipher-policy Attribute based encryption	Moderate
(Mollah et al., 2017)	Secure data sharing and searching at the edge of cloud network	Secure data sharing and searching	Secret key encryption, Public key encryption, Searchable secret key encryption and Digital signature	High
(Ali et al., 2015b)	Secure Data Sharing in Clouds (SeDaSC)	Secure Data Sharing, Access Control	Advanced Encryption Standard and symmetric encryption	High

Table 3
Comparison of related works towards secure offloading.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
(Al-Mutawa and Mishra, 2014)	Privacy preserving computational offloading	Privacy Protection	Data partition	High
(Dhanya and Kousalya, 2015)	Adaptive application partitioning and secure offloading in MCC	Secure Application Offloading	Application partitioning, dynamically changed the remote execution allocation	High
(Xia et al., 2015)	TinMan	Secure Offloading and Data Confidentiality	Trusted node, SSL session injection and TCP payload replacement	Medium
(Khan et al., 2015)	Cloud-manager-based re-encryption scheme (CMReS)	Secure Offloading and Privacy Protection	Both cloud and manager based re-encryption schemes	High
(Meng et al., 2015)	Security analysis of offloading under timing attacks	Defend Timing Attack	Modified cryptographic system	Low
(Saab et al., 2015)	Secure mobile application offloading mechanism	Secure Offloading	Profiling and decision making algorithm	High
(Duan et al., 2015)	Privacy preserving mobile application offloading	Secure Offloading	Adaptive data partitioning	High

own storage to improve security purpose. Almost a similar approach is presented in (Abdalla and Pathan, 2014). Here, the data is uploaded to the cloud service provider's end through a data protection manager which has two portions. One is data fragmenter that fragments the data and sends it to storage to multi-servers. The second one is data merger that merges the data while the user downloading from the stored data. The cloud service providers keep the full mapping information of fragmenting and merging data for individual mobile users. Multi-cloud technique is used in these approaches so that if somehow one cloud is compromised, the others remain safe and the unauthorized users cannot read or modify the full stored data. Authors in (Wang et al., 2014) propose a security approach to protect mobile user's data on media cloud. This approach is based on three parts such as secure sharing, scalable watermarking and Reed-Solomon coding. The secure sharing is used to upload multimedia contents in different pieces to different clouds and the watermarking is used for authentication purpose. Whereas, the Reed-Solomon error correction coding ensures the reliability of multimedia transmission over error-prone wireless networks. Here, the watermarking technique is utilized as it performs authentication in content level that has lower overhead than traditional authentication in packet level. Additionally, this paper utilizes scalable watermarking that adopted and scaled up or down under network bandwidth, mobile device's battery and display condition. In (Louk and Lim, 2015) and (Baharon et al., 2015), the authors present data security schemes for mobile users by homomorphic encryption. This encryption is considered one of the suitable and strong methods for security of stored data on the cloud. In ref. Khan et al. (2014), Abdul Nasir Khan et al. propose a cryptographic method that is block based sharing scheme (BSS) to ensure confidentiality and integrity of mobile users' stored data on clouds. In this method, in mobile device side, the security operations include logically dividing the data into multiple blocks, encryption and decryption operations of these blocks, and finally reconstructing to make original form. The cloud service provider offers data storage only. Finally, the authors implement and analyze the

performance that results the BSS has reduced computational intensive security operations than existing schemes, and also provides better security even the storage cloud is un-trusted. In (Gai et al., 2016), a novel data encryption approach is presented named Dynamic Data Encryption Strategy (D2ES). This approach utilizes a selective encryption strategy under required execution time requirements. Ref. Yang et al. (2015) presents an extended proxy-assisted approach that is based on attribute based encryption to provide scalable and fine-grained data sharing within clouds.

In (Yu et al., 2014), the authors propose a public auditing protocol to ensure integrity of user's stored data in cloud and shared data among the other users. In this protocol, asymmetric group key agreement scheme and proxy re-signature are used. The asymmetric group key agreement allows sharing group public and secret keys among group members, and creates tags for the files. And the proxy re-signature allows the mobile users to update the tags when the group members are changed. Moreover, this protocol preserves mobile user identity information secret by providing anonymity to the auditor and group members. In (Sookhak et al., 2017), the authors develop a remote data auditing method to verify the integrity of big data stored in cloud. This method is based on algebraic signature so that the auditor can check user's data possession in cloud. In addition, to extend this method, the authors design a new data structure, divide and conquer table (DCT), which supports dynamic data update operation. And using DCT, the user can perform data update operation at block level without downloading the full data. Finally, the authors implemented and analyzed the performance that results the algebraic signature and DCT have less computation-intensive operation on auditor and cloud than traditional data auditing methods. In ref. Yu et al. (2016), the data auditing mechanism utilizes zero knowledge proof systems, proxy re-signatures and homomorphic linear authenticators. And in (Tian et al., 2015), the authors propose a public auditing scheme based on dynamic hash table (DHT). The DHT is two-dimensional data structure deployed in third party auditor that records data property information for the purpose of

Table 4
Comparison of proposed schemes for secure virtualization.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
(Vaezpour et al., 2016)	SWAP, a security aware provisioning and migration approach	Protecting data leakage from phone clones	Dynamic allocation and migration of phone clones	High
(Hao et al., 2015)	SMOC, secure mobile cloud platform	Secure application cloning on VM	Hardware virtualization, a proposed file system	Moderate
(Paladi et al., 2016)	User security protection framework in cloud infrastructure	Data confidentiality within VM	Trusted VM launch protocol, domain based storage protection protocol	High
(Han et al., 2015)	An approach to protect co-resident attacks	Defending co-resident attacks	VM allocation policy	High
(Jin et al., 2015)	H-SVM, Hardware assisted secure VM	Protect guest VMs from malicious hypervisor	Hardware virtualization	High
(Liang et al., 2014)	A security isolation and migration approach for VM deployment	Secure VM deployment	Mandatory access control mechanism, security label in socket communication	Moderate

Table 5

Comparison of aforesaid related works for cloud based mobile application security.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
(Popa et al., 2013)	SMC, a security framework for mobile cloud applications	Ensure secure data communication within applications components and application integrity	Trusted managers, application signature verification	Moderate
(Tysowski and Hasan, 2013)	A protocol for secure mobile applications	Application security	Attribute based encryption, group keying mechanism and re-encryption	High
(Tang et al., 2015)	Strong API security for securing MCC	Web API security	Strong authentication, web signature, web encryption, public key infrastructure, transport layer handshake protocol	Moderate
(Zhang et al., 2009)	Secure elastic application model	Authentication, secure communication and migration	Trusted managers	High
(Tysowski and Hasan, 2011)	Secure communication model for highly scalable mobile application in cloud	Secure communication within application components	Key management in mobile device, cloud based re-encryption approach	High
(Tan et al., 2014)	STOVE model	Secure application execution	Trusted party, strong isolation and verification	High
(Zhong and Xiao, 2014)	MAACA, Mobile Application Assessment Cloud Architecture	Application security assessment	Trusted managers/components	Moderate

Table 6

Comparison of presented schemes counting privacy issues in MCC.

Works	Proposed Schemes	Security Features	Technical Approaches	Scalability
(Pasupuleti et al., 2016)	Efficient privacy preserving approach for outsourced data	Data Privacy	Probabilistic public key encryption and ranked keyword searching algorithm	High
(Bahrami and Singhal, 2015)	A lightweight data privacy preserving method	Data Privacy	Pseudo-random permutation method	Moderate
(Li et al., 2014)	An approach of privacy preserving data utilization	Data Privacy	Trusted proxy server	Moderate
(Zhang and Zhao, 2015)	A privacy preserving public auditing protocol	Privacy Preserving audit	chameleon hashing algorithm	High
(Zhang et al., 2014)	PASSQ, privacy assured substructure similarity query	Data Query Privacy	Secure index construction, trapdoor generation and query processing	Moderate
(Owens and Wang, 2013)	Data query privacy preserving for mobile mashups	Data Query Privacy	Dynamically created VMs as proxies, live migration of application level VMs	Low
(Niu et al., 2015)	CaDSA, Caching aware dummy selection algorithm	Location Privacy	Creating fake locations and sends with original information to query searcher	High
(Fawaz et al., 2015)	LP-doctor	Location Privacy	Trusted manager and analyzers	Moderate
(Chen et al., 2014)	LPDS, location privacy preservation scheme	Location Privacy	Distributed cache proxy servers	High
(Zhang et al., 2015)	Preserving location based information survey applications	Location Privacy	System level cloning of mobile devices	Moderate
(Park et al., 2013)	I2DM, improved identity management protocol	Identity Privacy	Pretty good privacy	High
(Khalil et al., 2014)	CIDM, consolidated identity management protocol	Identity Privacy	Trusted third party managers, extra layer of authentication	Moderate
(Khan et al., 2013b)	Identity privacy protection approach	Identity Privacy	Dynamic credential generations	High

rapid and dynamic auditing. In this auditing scheme, the auditing metadata excerpt the block tags transfers from service provider to the auditor, as a result, it minimizes the computational and communicational overhead. Moreover, to preserve privacy, this proposed scheme uses public key based homomorphic authentication and random masking created by the auditor.

Authors in (Qiu et al., 2016) propose proactive dynamic secure data scheme (P2DS) to ensure the mobile user's data protection from unauthorized access in cloud. This scheme is based on attribute based semantic access control and proactive determinative access algorithms. In (Jin et al., 2015; Odelu et al., 2016), the authors utilize cipher text-policy attribute based encryption (CP-ABE) to protect from unauthorized access. These schemes are referred as SL-CP-ABE (Secure and lightweight CP-ABE) and CP-ABE-CSCTSK (CP-ABE- constant size ciphertext and secret keys) respectively. These schemes provide access control in MCC environment and allow the mobile user to outsource securely computational processing to cloud from mobile devices with reduced encryption and decryption operation. Moreover, this scheme has no special restrictions on the access tree; therefore, the mobile users get flexible data access control. In ref. Li et al. (2016), the authors present 2SBM (IntercroSsed Secure Big Multimedia Model) to ensure secure assesses within different cloud platforms. This model is based on ontology based access recognition and semantic information matching algorithms.

Hongwei Li et al. Li et al. (2015) propose an efficient multi-keyword ranked search (EMRS) approach. This approach allows multi-keyword search over encrypted mobile user's data on cloud and also attains relevance-based result ranking. This approach is based on relevance score, secure k-nearest neighbor technique, an efficient index and blind storage system. The relevance score and k-nearest neighbor techniques in searchable encryption enable efficient multi-keyword ranked search, and return search results based on accuracy. The efficient index is used to enhance the search efficiency. And the blind storage system is used to conceal the access pattern of the search user within the cloud server. Ref. Guo et al. (2016) introduces a novel framework to ensure security and control access to searchable data/record. This framework is based on attribute based encryption technique. The authors in (D Liu et al., 2015) introduce personalized search over encrypted data and secure updates (PSU) in MCC. This search scheme is based on bloom filter, k-nearest neighbor technique, modified attribute based keyword search, and vector-space based search technique. The bloom filter and k-nearest neighbor techniques are used for efficient multi-keyword searching, and relevance based result ranking. The modified attribute based keyword search and vector-space based search technique allow attaining the search authorization for multi-data user scenario.

In (Zhang et al., 2016), Yinghui Zhang et al. propose an attribute based data scheme. This scheme is a hybrid mechanism combined with ciphertext-policy attribute-based encryption (CP-ABE) and symmetric encryption. The CP-ABE is suitable for cloud computing only but not for resource limited mobile devices as existing CP-ABE suffers intensive efficiency drawbacks due to large cipher size and computational overhead. But this proposed scheme has small and constant computational cost which is feasible for mobile devices. In (JK Liu et al., 2015), Joseph K. Liu et al. propose an infrastructure that provides mobile users to share and searching real-time video data securely. This infrastructure is based on some cryptographic functions such as Advanced Encryption Standard (AES), Searchable Symmetric Encryption (SSE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Digital Signature (DS). Firstly, the user registers with attribute based user secret key for video sharing purpose and also registers with cloud server for access control. Before uploading to the cloud, the video data is remarked with searchable keywords. Then, the video data encrypted using AES, searchable keywords are encrypted using SSE and finally, the CP-ABE is used to encrypt the AES keys under desired attributes. Ref. Yang et al. (2016) presents conditional proxy re-encryption (CPRE) scheme for cloud based secure data

sharing. In (Mollah et al., 2017), the authors introduce a proposed data sharing and searching scheme so that smart devices can share and search data securely at the edge of cloud. This scheme utilizes modern security tools like secret key encryption, public key encryption, searchable secret key encryption and digital signature. And in (Ali et al., 2015b), SeDaSC (Secure Data Sharing in Clouds) is proposed by Mazhar Ali et al. for both conversational cloud and MCC. This methodology has three entities such as user, a cryptographic server (CS) and the cloud. The user submits the data, group members list and access control list to CS. The CS is responsible for encryption, decryption, key management and access control. Firstly, the CS generates the symmetric key and encrypts the data by this. Next, the CS divides the key into two parts, one is for group members and other part is for access control purpose. Then, the encrypted data is stored in the cloud on behalf of the user. When a group member wants to download the data from the cloud, it sends the request with its key part to CS. Then, after authentication by CS, it allows to decrypt and download the data from the cloud to the requested user.

5.2. Security solutions for partitioning and offloading

In (Al-Mutawa and Mishra, 2014), a data partitioning concept is proposed to prevent mobile user's data exposure while offloading to remote and trusted or un-trusted entity. There are three steps in this concept. Firstly, the data is divided into non-sensitive and sensitive part based on user's preference. Then, the non-sensitive part is offloaded to the remote entity and the sensitive part is executed on the mobile device or trusted remote entity. Finally, the processed results are come back to the mobile device to make combination into final result. Here, the data partitioning concept is used to obtain the benefits of offloading while preserving privacy of user's sensitive data.

Ref. Dhanya and Kousalya (2015) proposes an adaptive application partitioning and secure offloading algorithm in MCC. This adaptive partitioning algorithm divides the application into sensitive and non-sensitive parts. The sensitive part is kept on mobile device for local execution, whereas the rest part of the application is offloaded to cloud for remote execution. The partitioned components are interconnected with each other. In this way, this adaptive partitioning algorithm provides secure offloading process. Moreover, for additional security, the entities for remote execute allocation are dynamically changed. Finally, the experimental evaluation results show that this adaptive partitioning and secure offloading algorithm is better than conventional linear programming based algorithms.

Authors in (Xia et al., 2015) propose TinMan to ensure data confidentiality and to perform security-oriented offloading from mobile device to cloud. In this approach, the sensitive data of mobile device are being separated from mobile applications and then, it is offloaded and stored to trusted node to reduce exposure. A trusted node is installed in VM on trusted cloud. The TinMan decides how efficiently and transparently execute this offloading procedure. The transparent Secure Socket Layer (SSL) session injection and Transmission Control Protocol (TCP) payload replacement are used for secure-oriented offloading and accessing to the sensitive data on trusted node.

In (Khan et al., 2015), Abdul Nasir Khan et al. propose a cryptographic method for secure offloading of mobile device's computational intensive operation to cloud. This method is named cloud-manager-based re-encryption scheme (CMReS) as it combines both characteristics of cloud based re-encryption and manager based re-encryption schemes. In this method, the encryption, decryption and re-encryption operations are distributed among mobile device, manager (a trusted entity), and cloud with preserving user privacy. Thus, it provides better security as well as minimum computational overhead. The manger is under the control of client organization and subject to handling the request from mobile client.

Tianhui Meng et al. Meng et al. (2015) propose a model to defend against timing attacks during offloading process in MCC. In timing

attack, the attacker presumes information about private key from runtime measurements of successive requests. This timing attacks are not defended properly by using traditional cryptographic techniques. However, this proposed model is based on two techniques: (a) in mobile offloading process, a master key storing in cloud side where the attacker get offloading services, and (b) the probability of timing attacks decreasing by changing frequently the keys. Finally, the authors compute the security and cost tradeoff to achieve this model as a better secure offloading with minimum cost.

Authors in (Saab et al., 2015) propose a secure and energy efficient mobile application offloading mechanism in cloud environment. This mechanism consists of profiling, decision making and offloading engine. The profiling and decision making algorithms are responsible for dynamic partitioning of mobile application to make optimized energy consumption and security measures. After decision making the full or partial part are offloaded to cloud through offloading engine. Yue Duan et al. (Duan et al., 2015) propose and experiment a privacy preserving mobile application offloading approach. In this approach, user's privacy related information is kept within mobile device during offloading. The offloadable codes are identified and offloaded automatically by dynamic decision making algorithm. The experiment result shows this proposed approach preserves privacy during offloading process with energy savings.

5.3. Security solutions for virtualization related challenges

Seyed Yahya Vaezpour et al. (Vaezpour et al., 2016) propose SWAP, a security aware provisioning and migration scheme, for phone clones. The phone clone is a thin VM on cloud where mobile device is cloned that supports to offload the computational intensive data and application for processing. The SWAP includes two techniques such as secure phone clone allocation to reduce the threats of data leakage from VM, and migration of phone clone if the threat becomes high.

In (Hao et al., 2015), a secure mobile cloud platform, referred SMOC, is presented by Zijiang Hao et al. This platform enables the mobile user to clone securely of its operating system as well as applications to VM on cloud. To ensure user data security on mobile device, hardware virtualization technique is used that allows to isolate the data and application processing from local mobile device's operating system. Moreover, a file system extension is introduced so that the applications can be migrated into VM for higher security or processed within the mobile device for getting better user experience.

Authors in (Paladi et al., 2016) present a security framework for cloud infrastructure. This framework includes a trusted VM launching and a domain based stored data protection protocols. The trusted VM launching protocol is used before deploying guest VMs, the trust is established by remotely attesting host platform configuration. Whereas, the domain based storage protection protocol ensures data confidentiality in remote storage by using cryptographic methods.

In (Han et al., 2015), Yi Han et al. propose an approach to defend against co-resident attacks in cloud computing. This approach is based on improved VM allocation policy to make difficulties for attackers to co-locate on VMs. Finally, the authors implement this allocation policies on simulation platform CloudSim that results this solution minimizes the probability of attacker's co-location with their targets.

Authors in (Jin et al., 2015) present H-SVM which is a hardware-assisted secure VMs. This approach protects the guest VMs from malicious hypervisor by memory virtualization. Due to utilizing hardware based memory virtualization, this proposed mechanism is less vulnerable than software based virtualizations.

Ref. Liang et al. (2014) propose a lightweight security approach to secure VMs deployment. This approach utilizes mandatory access control mechanism in VM deployment to control the available resources, and provide strong isolation among guest VMs. Moreover, in this approach a security label in socket communication is introduced to secure VM migrations. Finally, the experiment results outcome of

this approach is effective in isolation and migration with low computational overhead.

5.4. Security solutions for mobile cloud applications

A security framework for cloud based mobile applications is proposed in (Popa et al., 2013) named Secure Mobile Cloud (SMC). In this framework, it is presented to ensure the security in data communication within the components of an application running on both mobile device and cloud, and the integrity of an application during installation, processing or updating in mobile devices. There are some security components installed in the cloud and mobile device ends to ensure application integrity and data confidentiality. To verify the integrity of application, firstly, the application existence is verified by searching its name on application stores. Then, the application signature is compared with the original one that has been found in application store. If both signatures are found same, it can be said that there is no malicious codes attached with the application. There are six security managers discussed in this framework such as the mobile manager, the mobile security manager, the cloud security manager, the optimization manager, the application manager and the policy manager. Here, the mobile manager collects the events happening in mobile device and transfers these to analyze to concerned manager, the mobile security manager confirms the arrangement of security properties in the mobile device, the cloud security manager confirms the arrangement of security properties in the cloud, the optimization manager collects the information from different sensors and transfer it to mobile manager, the application manager checks the integrity of application, and the policy manager determines the requirement of security components for a particular security level.

Authors in (Tysowski and Hasan, 2013) propose a hybrid attribute and re-encryption based protocol for secure mobile applications in cloud computing environment. This protocol utilizes attribute based encryption, a group keying and re-encryption techniques. The attribute based encryption is revised so that the key generation responsibility is distributed between mobile device and trusted entity. Thus, the mobile device is mitigated from the computational overheads. Whereas, the group key mechanism provides extra security by creating a group secret key which is shared secretly among particular user or group. And the re-encryption is a process of encryption of the stored cipher to allow efficient revocation of mobile users. This process is administrated by a trusted entity. In (Tang et al., 2015), Longji Tang et al. present a token based three factor strong Application Program Interface (API) security model. These are (a) basic authentication including API user registration with strong password protection, (b) modern security mechanisms such as message level security, web signature and web encryption, and (c) security mechanism within API and its backend services as a third security factor such as token based API for backend authentication, public key infrastructure and transport layer handshake protocol.

Xinwen Zhang et al. (Zhang et al., 2009) propose a secure elastic mobile application model for cloud computing. The security targets include authentication, secure communication and migration within application components in both mobile device and cloud. In this approach, the key components are device elasticity manager, cloud manager and application manager. The device elasticity manager is responsible for locating the application components and selecting the paths to communicate within the components securely. The cloud manager allocates the resources and maintains computational, bandwidth and storage usage information for different parts of components running in the cloud end. The application manager located in the cloud allows to install and launch the application components in different cloud nodes. Here, the application components are referred as a weblets.

Authors in (Tysowski and Hasan, 2011) presents three key distribution schemes such as identity-based encryption, multi-level key management and data re-encryption, and a cloud based re-encryption scheme to provide secure communication of scalable mobile applica-

tions within cloud computing. In this scheme, the user key management is done by the mobile device due to trusted purpose, whereas the computational intensive re-encryption processing is performed by the cloud.

A model named STOVE (Strict, Observable, Verifiable Data and Execution) is presented in (Tan et al., 2014) for untrusted mobile application execution securely. When an untrusted application runs and executes, it does not able to harm other applications or operating system, and does not access any un-authorized application or data. This model works with three steps. In first step, the STOVE strictly limits and totally isolates the untrusted applications from other application in where it runs. In second step, STOVE verifies the strictly isolated code by formal verification methods. Lastly, STOVE executes all data access in favor of the untrusted application in order that all data access is observable.

Authors in (Zhong and Xiao, 2014) propose a cloud based mobile application security assessment framework named MAACA (Mobile Application Assessment Cloud Architecture). This framework consists of five components such as frontier interface, service manager, service data center and analysis engine. As this framework is cloud based, the componets are implemented in the cloud end. The frontier interface is used to upload the mobile application for assessment and provide interface for users to check assessment reports. The service manager receives the assessment request from frontier interface and sends it with user information to analysis engine after authentication. The service data center stores all necessary data for assessment operation such as user information, requirements, authentication information and user's historic assessment report. The last component is analysis engine that performs uploaded application assessment, and after completing, the assessment report sends to service data center for record.

5.5. Secure mobile cloud architectures

In (Xiu-feng et al., 2011), Qiu Xiu-feng et al. propose a secure architecture for MCC. This architecture is considered modern mobile and cloud computing security threats, features of mobile internet, and other secure cloud architectures. The whole architecture is divided into five parts. In first part, there are some resources to ensure security and privacy such as data and privacy protection, cipher text data query, validation of data integrity, content security services, and early informing of security events. Second part contains some resources to ensure security of platform services, and virtualization such as VM segregation, secure VM monitoring, secure VM migration and secure VM mirror. Third part has different levels of security service for cloud infrastructure due to the security requirements is different from one user to another, and the infrastructure is built-up and connected with mobile communications. In fourth part, a cloud security management platform is designed to manage the users and keys, authentication and authorization, anti-malware, security logging and audit. This security management platform assists all layers of this architecture, secure cloud platform and infrastructure, and contains various security domains. In fifth part, the architecture provides cloud services and applications through wireless access with ensuring security and protection by customizing security services. And last part includes and supports the agreements, permissions and compliance check according to different cloud security standards and regulations. Before installing an application, the cloud service providers test and evaluate the application by trusted third parties to measure the security risks and trust levels. Thus, the cloud service users do not face any unnecessary loss and difficulties from over-measured trust level. This trust level measurement also reinforces to cloud service providers to increase the security services and quality.

Authors in (Dey et al., 2015) present a context-aware security architecture for MCC that needs to be deployed at cloud end as an additional security layer. This architecture contains a check point to

confirm incoming traffic patterns, a learning algorithm to learn from previous attacks, an adaptive module to prevent DoS attacks, an outer cloud module to maintain the mobile clients by receiving authentic requests, and establish a secure session between mobile client and cloud.

A secure MCC architecture is proposed in (Olafare et al., 2015) that consists of some components installed in both mobile device and cloud. The components in mobile device are mobile manager, optimization manager and mobile security manager. And the cloud side components include application manager and cloud security manager. Each component has particular functionalities. This architecture is presented to guarantee the integrity of application and the communications among same application parts in both mobile and cloud ends.

In ref. Horrow et al. (2012), Susmita Horrow et al. propose a secure cloud architecture to provide mobile infrastructure as a service to mobile users. This architecture has several components such as mobile client, cloud admin and private cloud infrastructure. The cloud admin is responsible for authentication the mobile user, receiving the user request, managing the resources in VMs, user isolation in cloud and packet filtering. When a user requests for resources, the cloud admin creates a template in VM and a virtual network so that mobile user can use resources securely. When multiple requests are come to cloud admin, it enforces to isolate the users within virtualized cloud environment.

Authors in (AlShahwan et al., 2015) propose a security framework for RESTful MCC services. This framework is based on existing security and key management protocols. This framework includes different modules and blocks such as web service servlet, HTTP listener, request handler, parser module, fuzzy logic module, augmented offloading module, orchestrator module, response composer, certificate generation and authorization modules.

Payal Patel et al. Patel and Patel (2015) propose a security framework for CloneCloud based MCC architecture. This security framework utilizes the elliptic curve cryptography (ECC) and blowfish algorithm to ensure authentication and confidentiality within mobile device and cloud server. The ECC technique is public key based which utilizes algebraic structure of elliptic curve user finite fields. This technique is used for launching secure communication channel for key exchange. The blowfish algorithm is sixty-four-bit symmetric block cipher of feistel network that iterates encryption process sixteen times. In this security scheme, the ECC is used for key exchange, and the blowfish algorithm is used for data encryption.

5.6. Authentication to mobile cloud

The authentication is essential for mobile users to avail the cloud based services and it eliminates the various attack risks during accessing to the services. But authentication within the edge-cloud based architectures is complex compare to MCC as in these architectures there is an extra-tier such as cloudlets, fog servers, micro-cloud etc. However, there are several knowledge based, token based, image based, biometric based and behavioral biometric based authentication techniques are available. Among them the knowledge based authentication techniques are widely used. But it is more insecure than others and vulnerable to different types of attacks like dictionary attacks, brute force attacks, phishing attacks etc. The biometric and image based authentication techniques are more secure than knowledge based authentication technique. But the problems with biometric authentications are these require extra devices which are unpleasant to use.

There are several works have been done towards mobile user authentication to cloud. A privacy-aware authentication scheme is proposed in (Tsai and Lo, 2015) to ensure security to cloud service users so that mobile users can access many services from different service providers by using a single private key. This approach strengthen its security by utilizing bilinear crypto system and dynamic nonce

generation. Moreover, it supports mutual authentication, key exchange, user anonymity and user untraceability. But to implement at trusted smart card generation (SCG) and service provider end, it does not require any verification tables. Here, the trusted SCG is used to distribute the keys among distributed clouds and mobile users, but it does not engage in individual mobile user authentication process. In each user authentication session, the targeted cloud server only interacts with the requested user. Therefore, it results reduced authentication processing time and usage of memory spaces.

Authors in (Rassan and AlShaher, 2014) proposes and implements a biometric based authentication approach to protect the unauthorized access to cloud. The authors use fingerprint recognition technique for biometric identification. The authors use the mobile device's camera as a biometric sensor instead of external device for the purpose of simplicity. In algorithm section, firstly, the mobile device's camera takes fingerprint image samples of user and then, extract the features. Next, these features store in the database for future usage. Another biometric based authentication scheme for multi-cloud environment is introduced in (Kumari et al., 2017). In this scheme, to enhance the accuracy of biometric pattern matching, the authors utilize bio-hashing techniques.

In (Jeong et al., 2013), Young-Sik Jeonget al. propose an efficient and user convenient multi-factor based mobile device authentication approach. The multiple factors used in this approach include mobile device's identity, username/password and user bio information like voice or face. This approach can enhance the security by requiring this authentication process before entering to the cloud services through multi-factor authentications. And it also enhances the authentication efficiency by processing the authentication factors one by one on VMs in cloud. Moreover, for authentication efficiency, VMs in services process the authentication of individual authentication factors so that the time necessity for authentication would not increase even if the number of authentication factors increased.

In (Dey et al., 2014), the authors propose an authentication scheme named MDLA (Message Digest and Location based Authentication). In this scheme, mobile user is authenticated to cloud by message digest created by cloud server, location and timestamp. The advantages of this scheme include the mobile user does not need to memorize any password, and the cloud server performs resource intensive parts like registration, authentication and updating the authentication parameters. Therefore, security and performance analysis shows that this scheme provides better security and low power consumption than other schemes.

Authors in (Bouzefrane et al., 2014) propose an authentication approach for cloudlets based architecture. In this approach, the near field communication (NFC) enabled mobile devices authenticate cloudlets by using its NFC before computational offloading process. In (Donald and Arockiam, 2015), a framework named mobile cloud authenticator (MCA) is presented to authenticate mobile users in MobiCloud based architecture. In this framework, a unified cloud authenticator (UCA) is proposed that placed in-between mobile device and cloud. This UCA supports to authenticate both mobile user and cloud server by registration, authentication and verification processes.

5.7. Security solutions for mobile devices

In this section, we present the security solutions which are related to physical threats, storage and malwares. Furthermore, we present cloud based and on-device security applications.

5.7.1. Solutions for physical threats

The application developers should pay their attention in two issues such as they can add a security layer as an extra in application level when the users keep and access to their sensitive data, and they can ensure that users' sensitive data do not store in identity module card. In addition, cloud backup services are important for users and when a

user's mobile device get lost or data lost, then, the user can recover his data from the cloud. Currently, the special security features are built on mobile devices. The Google device policy application (Online, 2016) provide a special feature for mobile users that after stealing or getting lost the mobile device, the data inside the device is cleared as well as the device is locked remotely. Some other approaches like protection of cloud data access and protection of device identity can be integrated for increasing the security of both mobile device and cloud.

5.7.2. Solutions for malwares

To protect and prevent attacks by malwares on mobile devices, there are two kinds of security applications are available for mobile devices, i.e., cloud based (Walls and Choo, 2015) and on-device application (Imgraben et al., 2014). Several advantages of cloud based solution over on-device applications such as better detection and prevention, reducing on-device resource consumption and application complexity. The on-device security applications are widely popular to detect and prevent malwares but considering long term, these applications are not properly effective for modern complex malwares and threats.

5.7.3. Available on-device security applications

There are several security applications available for mobile devices with different features like detect and prevent mobile malwares, control unauthorized access and protect privacy. Some on-device security applications are 360 Degree Mobile Security (www.360safe.com), Avast Mobile Security (www.avast.com/free-mobile-security), Norton Mobile Security (www.mobilesecurity.norton.com/), Kaspersky Mobile Security (www.kaspersky.com/android-security), ESET Mobile Security (www.eset.com/us/home/products/mobile-security-android/), Lookout Mobile Security (www.lookout.com/android) and so on.

5.7.4. Malware detection techniques

At present, many works have been done towards detecting, defending, monitoring, and analysis of the malwares from both academic and industries. In (Suarez-Tangil et al., 2014), Guillermo Suarez-Tangil et al. organize several malware detection techniques in their paper. The techniques are based on following features.

- 22) *Detection Types*: According to code analyzing approach, there are two kinds of detection techniques are available such as static analysis and dynamic analysis. The static analysis technique is vastly used to find out suspicious strings and comparatively fast technique. In this technique, the malicious codes are detected by unpacking and decompiling the application process. On the other hand, the dynamic analysis technique identifies the malicious activities by installing and running the application on an emulator or a device.
- 23) *Monitoring Types*: The monitoring technique gathers user, kernel and hypervisor level activities depending on feature type that are extracted. The collection of monitoring techniques is system calls, network activity, event logs, user activity, instructions, permissions and program traces.
- 24) *Analysis Types*: After monitoring, it needs to analyze the data if there present any malware. Several types of analyzing techniques are available such as clustering, support vector machines, self-organizing maps, machine learning algorithms, control flow graphs, data flow graphs and program dependency graphs.
- 25) *Identification Types*: The detection types can be anomaly, misuse or specification based system subject to the identification types. This is the main guiding feature to identify the malwares, and it also use in intrusion detection system.
- 26) *Identification, Analyzing and Monitoring Places*: The identification, analyzing and monitoring tasks utilize heavy resources of mobile devices, and it does not suitable for mobile devices. Thus, there is a trend to offload the processing to cloud. However, some

part of tasks also takes place on the mobile devices.

5.7.7. Cloud based solutions

The anti-malware applications are used for detecting and preventing the malicious applications and threats on mobile devices. However, due to having limited resources of mobile devices, the anti-malware applications, security applications, or monitoring tools are not feasible to run on these devices. However, to address these issues, the computational outsourcing, offloading or cloud based solutions are fit for mobile devices. In (Hurel et al., 2015), the authors propose an approach to provide cloud based security functions for mobile devices. In this approach, an openflow switch is integrated with mobile device for redirection purposes. A security manager and openflow controller module are installed on the cloud side. During mobile devices connecting and communicating with remote destinations, all the data passes through the openflow controller. Authors in (Zonouz et al., 2013) propose a cloud based lightweight security solution for mobile devices named Secloud. The Secloud architecture consists of three components such as mobile client agent, emulator and proxy server. The mobile client agent is an application that runs on mobile device after completing registration from Secloud. The emulator is installed on VM of cloud where the full system of mobile device is copied and synchronized. The proxy server makes mirror of the network traffic of mobile device and sends it to the emulator. When any kind of security compromises are detected within emulator, it instant informs to the mobile client agent to take actions like remove the infected files or close the attacker's network connections. In (Jarabek et al., 2012), it is presented a cloud based anti-malware system named ThinAV for mobile devices. The ThinAV consists of two components such as a mobile client application and a ThinAV server. The mobile client application allows offloading applications of mobile device to ThinAV server. The ThinAV server sends it to the third-party malware scanning entity and returns the scanning results to the mobile client. For faster returning the scanning result, the ThinAV server caches scan results. Authors in (Alam et al., 2014) present an in-cloud malware analysis and detection system called lightweight anti-malware engine (LWE). This LWE has three layers such as a lightweight agent, a lightweight anti-malware engine and in-cloud anti-malware engine. The lightweight agent and anti-malware engine both are malware analyzer and detector. But the lightweight agent is based on simple signature based technique, whereas, the lightweight anti-malware engine is more complicated than the first one which is installed in mobile device end. However, if any malware or suspicious activities cannot be detected and analyzed at the first two layers, then, in-cloud malware engines take necessary actions. Therefore, due to three layered detection and analysis, this LWE becomes faster than other approaches. In ref. Shi et al. (2015), Yue Shi et al. propose cloudlets based security functions to detect malwares of mobile devices. These cloudlets are connected with remote cloud. With the help of cloud, the cloudlets are updated its malware database. Moreover, a trusted chain is established among mobile device, cloudlets and remote cloud, and an inter-cloudlets protocol is introduced to enable distributed malware detection.

5.7.8. Mobile devices storages issues

To protect data confidentiality and privacy, there needs to ensure the security of mobile device storages. To ensure mobile device storage, it can be utilized by two approaches (a) using encryption of data and securing the encryption key by using Trusted Platform Module which is installed in a stand-alone chip on mobile device, and (b) using cloud services by users to store all data within it.

5.7.9. Authentication to mobile devices

Several authentication mechanisms to mobile devices are available such as PINs, graphical passwords, fingerprint scan etc., but these commonly used authentication mechanisms have some limitations.

One important limitation is one-time authentication. Hence, after login, the unauthorized user cannot be authenticated. In (ElMenshawy, 2015), Dina El Menshawy et al. propose a touch screen pattern based authentication scheme. This scheme is combined with PIN and touch behavior on the mobile device's screen. Authors in (De Luca et al., 2013) introduce a back of device (BoD) authentication approaches such as BoD pattern unlock and BoD shapes where the back of mobile device is used for input purpose. The BoD input for authentication makes users more convenient, less input time consuming and secure against different types of attacks like shoulder surfing attacks. Usually, a shape consists of random number of horizontal and perpendicular strokes. The authors claim after completing a user experience survey that this approach is faster, easier to memorize, more secure, and improved than other authentication approaches. However, for continues authentication of the mobile user, Zdeňka Sitová et al. Sitová et al. (2016) propose a set of behavioral biometric features. This set includes hand movement, orientation and grasp. By using accelerometer, gyroscope and magnetometer to unobtrusively take subtle micro-movement and orientation patterns generated when the user grasps, holds and taps on the mobile device. Ref. Zhao et al. (2013) introduces a biometric behavior based continuous authentication approach named GTGF (graphic touch gesture feature). In this approach, the authors use GTGF to extract and find out the identity from touch traces. The intensity values and shapes show up the touch traces' movement and pressure dynamics. To achieve this authentication approach's usability, a database of gesture is formed from six commonly used touch gestures. Authors in (Feng et al., 2013) introduce a continuous mobile authentication approach named TAP (typing authentication and protection). This approach is based on virtual key typing biometrics. The biometric information includes typing habit and hand morphology.

5.8. Security solutions for privacy

In (Pasupuleti et al., 2016), the authors propose an approach that preserves privacy of mobile device's outsourced data in cloud. Probabilistic public key encryption technique and ranked keyword searching algorithm are utilized here. Firstly, the mobile user makes an index for file collection, and before sending for storing in the cloud, it encrypts both the data and index. Then, to access the stored data in the cloud, the user produces trapdoor for keywords and sends to the cloud. When the cloud receives the trapdoor, the cloud starts to search for a list of matched data entries and its corresponding encrypted relevance scores. Next, after collecting, the matched data is sent back to the user in ranked sequences which are based on the relevance scores. Finally, the user can retrieve the original data back by decryption operation. In (Bahrami and Singhal, 2015), a lightweight cryptographic method for mobile device is proposed to store data on clouds. This method is based on pseudo-random permutation operation. As it is light-weight, the permutation operation is done on mobile device instead of cloud in order to protect data privacy. In ref. Li et al. (2014), a privacy assured data utilization technique in cloud is proposed. Here, a private cloud is introduced that is used as a proxy to support privacy preserving keyword searching and access control over encrypted data on public cloud.

Authors in (Zhang and Zhao, 2015) propose an identity privacy preserving public auditing protocol that is based on the chameleon hash signature algorithm. In this protocol, the user randomly generates a pseudo-key pair and compute data tag with this pseudo-key pair to hide user identity. Thus, the cloud server cannot differentiate the actual origin of the outsourced data.

In (Zhang et al., 2014; Owens and Wang, 2013), two data query privacy preserving approaches for MCC are presented. The authors in (Zhang et al., 2014) propose privacy assured substructure similarity query (PASSQ). This proposed solution contains three algorithms such as secure index construction, trapdoor generation and query proces-

sing. The secure index converts original into encrypted form to conceal the information. And last two algorithms are used to perform privacy assured similarity calculation and trapdoor generation respectively. The authors in (Owens and Wang, 2013) propose an approach to preserve data query privacy for mobile mashups in MCC. There are two kinds of mechanisms are presented, one is for server side and another is for mobile client side. In server side mechanism, dynamically created VMs are used as proxies to protect data privacy within the communication between mashup server and mobile device. And in mobile client side, live migration is held from application level VMs to cloud to conceal data collection as well as aggregation procedures from eavesdropper.

To protect location privacy, there are several efforts have been proposed. Among them, K-anonymity (Sweeney, 2002) is the most popular model. However, it wastes network bandwidth and extra overhead in both mobile device and server. Other recent efforts are presented in (Niu et al., 2015; Fawaz et al., 2015; Chen et al., 2014; Zhang et al., 2015). In (Niu et al., 2015), the authors propose a caching aware dummy selection algorithm (CaDSA) to improve location privacy of mobile users. In this algorithm, the mobile device sends some fake location with real location information as query parameters to location based service providers. Thus, the service provider cannot realize the user's real location among the fake ones. In (Fawaz et al., 2015), Kassem Fawaz et al. propose a fine-grained location access control tool, named LP-doctor, to prevent location privacy threats from location access of mobile applications. This LP-doctor is mobile device level tool that enables the users to utilize the operating system (OS) based location access control but without any modification of application layer or OS. It has several components with specific functions such as application session manager, policy manager, place detector, mobility manager, threat analyzer and anonymization actuator. The application session manager monitors application launch and exit events to anonymize location. The policy manager maintains a privacy policy for currently visited place and launched applications. The privacy policies included three possible actions like block, allow and protect which are specified by the users to be applied for the application. The place detector monitors the user's current location, and the mobility manager updates user location profile when the user changed its location. The threat analyzer decides whatever to allow the user location or not according to policy manager applied by the user. If the threat analyzer decides to protect the location information, then anonymization actuator takes necessary actions by adding a fake location to ensure location anonymity. Finally, this LP-doctor is implemented and evaluated its performance that results LP-doctor can mitigate location privacy threats with little effect of usability and quality of services. Authors in (Chen et al., 2014) propose LPPS (location privacy preservation scheme) to protect location privacy of mobile users. This scheme introduces a distributed cache proxies to store users frequently visited locations those are divided into groups, and pushing the desired location data from group to particular mobile users. If data is available in cache, the user does not communicate with the location based servers to send out location related queries. This result preserves the location privacy. Ref. Zhang et al. (2015) introduces a privacy protection in location based information survey applications (LB-ISA). This scheme utilizes cloud infrastructure in where the mobile device is system level cloned. The computing of distributed function is dynamically allocated among the cloud clones through peer to peer network. This computing is privacy preserving as the cloud clone has more system resource access than mobile device. Numerical simulation results this scheme has good load-balancing, low communications overhead and cost with better privacy protections in LB-ISA.

The authors in (Park et al., 2013; Khalil et al., 2014; Khan et al., 2013b) present approaches to protect mobile user's identity privacy in MCC. In (Park et al., 2013), In-Shin Park et al. introduce an improved identity management protocol (I2DM). This protocol uses pretty good

privacy (PGP) that based on public key infrastructure (PKI). This PGP allows mutual dependence based communication and proper mobile user identity management. Authors in (Khalil et al., 2014) propose a consolidated identity management (CIDM) architecture that protects mobile user identity from three possible vulnerabilities such as privacy leakage from identity management server, compromising mobile devices and interception of network traffic in MCC. In this CIDM architecture, the identity management (IDM) is a third-party server that manages mobile user's digital identities on behalf of service provider. The protection procedure includes three steps such as (1) separating authorization credentials, and distributes among the user, IDM server and service provider to protect illegal access from IDM compromising or traffic interception, (2) adding an extra layer of authentication to prevent mobile device compromising, and (3) consolidating the security of the communication link between the CIDM and the cloud service provider to decrease the probability of successful compromising of that link. In ref. Khan et al. (2013b), the proposed approach is based on dynamic credential generation instead of digital credential method. The dynamic credential operation is outsourced to third party entity to minimize the computational overhead of mobile devices. Moreover, to improve the performance and security of this approach, the credential information of mobile devices are frequently updated according to packet exchange between mobile device and cloud. The generation of dynamic credentials is on the basis of communications between mobile device and the cloud to ensure better protection from credential stealing attacks. This scheme has three entities such as mobile user, cloud service provider and manager. To ensure authorized mobile user, the manager first authenticates the user, and then, forwards the dynamically generated credentials. And these credentials are encrypted with user public key to guarantee confidentiality.

6. Open issues

The security and privacy challenges discussed in Section 4 clarify that the MCC not only retains the contemporary security and privacy concerns but also entails a new class of challenges from the emerging usage of such a new technology. In addition, the present challenges become more difficult to handle for the integration of mobile device and cloud as data, application, virtualization and remote execution become more vulnerable to threats when the direct control of users over the data, application and virtualization is absent.

In Section 5, we present several recent security and privacy related works. But despite intensive research efforts, there are still open issues which need to be solved for giving a secure and privacy preserved MCC environment. Firstly, a comprehensive and integrated security solution is needed to develop that enclose most of the major security requirements as mentioned in Section 3. Most of the proposed solutions are dependent on particular requirements/challenges. But it is not cost effective to deploy and configure a lot of security issues in a MCC environment simultaneously with the existing technologies. Moreover, an integrated solution will result in easy management, and provide desired security level.

Since application partitioning, offloading and remote executions require data communication between mobile device and cloud, more focus is needed to ensure security in this area. To reduce performance degradation, all operations do not necessarily use encryption method especially in computational offloading and remote execution. Therefore, the attackers can make a target to memory locations inside and outside of the processors where data is stored temporarily. Hence, some solutions are required which ensure security while performing these processing. Moreover, the data recovery in case of data loss is also needed to focus.

Phone clone, a thin VM, is an essential part of MCC virtualization where the mobile devices are cloned at cloud for data and application processing. Since phone clone at virtualized environment poses secur-

ity threats to mobile users, security and privacy for phone clone is one of the important challenges for MCC. At present, there are only a few works in this area and required lot to do. Moreover, the mobile users want to migrate their own data and application from mobile devices to phone clones due to its storage and resource constraints. However, these migrations impose some technical challenges. A flexible framework is needed that allows the mobile users to migrate their data and application to mobile clones easily and securely.

Finally, the security solutions provide advantages to both mobile users and service providers, but they introduce computational and communicational overhead. The resource limited mobile devices suffer from these overheads on its performance. Hence, the proposed security solutions should encounter both security requirements as well as performance.

7. Conclusions

In this paper, we present a comprehensive survey of security and privacy challenges, and their security solutions of MCC. Firstly, we provide a background overview of MCC. Then, we discuss the potential security and privacy challenges of MCC. Next, we present very recent related works along with security solutions, and summarize the solutions in tabular format so that the readers in this field can compare, analyze and direct further research activities. However, although this research field is still immature and unexplored in depth, many security and privacy related challenges are still under research, and yet to be solved. Hence, finally, we discuss some open issues in this regard. We hope that this paper will be beneficial in giving a hint the way ahead, and enable a massive integration of mobile computing and cloud computing.

References

- [Online: 2016] Locations of Google's Data Centers: (<http://www.google.com/about/datacenters/inside/locations/index.html>).
- [Online: 2016] Locations of Google's Data Centers: (<http://www.royal.pingdom.com/2008/04/11/map-of-all-google-data-center-locations/>).
- Ab Rahman, N.H., Cahyani, N.D.W., Choo, K.K.R., 2016. Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurr. Comput.: Pract. Exp.* Abdalla, A.-k.A., Pathan, A.-S.K., 2014. On protecting data storage in mobile cloud computing paradigm. *IETE Tech. Rev.* 31, 82–91.
- Ahmed, E., Gani, A., Khan, M.K., Buyya, R., Khan, S.U., 2015. Seamless application execution in mobile cloud computing: motivation, taxonomy, and open challenges. *J. Netw. Comput. Appl.* 52, 154–172.
- Alam, S., Sogukpinar, I., Traore, I., Coady, Y., 2014. In-Cloud Malware Analysis and Detection: State of the Art. In: *Proceedings of the 7th International Conference on Security of Information and Networks*, p. 473.
- Ali, M., Khan, S.U., Vasilakos, A.V., 2015a. Security in cloud computing: opportunities and challenges. *Inf. Sci.* 305, 357–383.
- Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., et al., 2015b. SeDaSC: Secure data sharing in clouds. *IEEE Syst. J.* 99, 1–10.
- Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K., 2016. Authentication in mobile cloud computing: a survey. *J. Netw. Comput. Appl.* 61, 59–80.
- Alizadeh, M., Hassan, W.H., 2013. Challenges and opportunities of mobile cloud computing, in *Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013. 9th International, pp. 660–666.
- Al-Mutawa, M., Mishra, S., 2014. Data partitioning: an approach to preserving data privacy in computation offload in pervasive computing systems. In: *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, pp. 51–60.
- Alqahtani, H.S., Kouadri-Mostefaou, G., 2014. Multi-clouds Mobile Computing for the Secure Storage of Data, in *2014 IEEE/ACM. In: Proceedings of the 7th International Conference on Utility and Cloud Computing*, pp. 495–496.
- AlShahwan, F., Faisal, M., Ansa, G., 2015. Security framework for RESTful mobile cloud computing web services. *J. Ambient Intell. Humaniz. Comput.*, 1–11.
- Amin, M.A., Bib Abu Bakar, K., Al-Hashimi, H., 2013. A review of mobile cloud computing architecture and challenges to enterprise users, in *GCC Conference and Exhibition (GCC)*, 2013. 7th IEEE, pp. 240–244.
- Arabo A., Pranggono, B., 2013. Mobile Malware and Smart Device Security: Trends, Challenges and Solutions, in *Control Systems and Computer Science (CSCS)*, 2013. In: *Proceedings of the 19th International Conference on*, pp. 526–531.
- Azfar, A., Choo, K.-K.R., Liu, L., 2016. Android mobile VoIP apps: a survey and examination of their security and privacy. *Electron. Commer. Res.* 16, 73–111.
- Ba, H., Heinzelman, W., Janssen, C.-A., Shi, J., 2013. Mobile computing-A green computing resource, in *Wireless Communications and Networking Conference (WCNC)*, IEEE, pp. 4451–4456.
- Baharon, M.R., Shi, Q., Llewellyn-Jones, D., 2015. A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing, in *Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, 2015 IEEE International Conference on, pp. 618–625.
- Bahrami, M., 2015. Cloud Computing for Emerging Mobile Cloud Apps, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2015. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 4–5.
- Bahrami, M., Singhal, M., 2015. A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2015. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 189–198.
- Bouzeffrane, S., Mostefa, B., Amira, F., Houacine, C., Gagon, H., 2014. Cloudlets Authentication in NFC-Based Mobile Computing, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2014. In: *Proceedings of the 2nd IEEE International Conference on*, 2014, pp. 267–272.
- Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I., 2009. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.* 25, 599–616.
- Cahyani, N.D.W., Martini, B., Choo, K.K.R., Al-Azhar, A., 2016. Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study. *Concurr. Comput.: Pract. Exp.*.
- Cai, Y., Yu, F., Bu, S., 2014. Cloud computing meets mobile wireless communications in next generation cellular networks. *Netw. IEEE* 28, 54–59.
- Cai, W., Zhou, C., Li, M., Li, X., Leung, V., 2015. MCG Test-bed: an Experimental Test-bed for Mobile Cloud Gaming. In: *Proceedings of the 2nd Workshop on Mobile Gaming*, pp. 25–30.
- Chard, K., Caton, S., Rana, O., Bubendorfer, K., 2010. Social cloud: Cloud computing in social networks, in *Cloud Computing (CLOUD)*, 2010. IEEE In: *Proceedings of the 3rd International Conference on*, pp. 99–106.
- Chen, F., Zhang, C., Wang, F., Liu, J., Wang, X., Liu, Y., 2015. Cloud-assisted live streaming for crowdsourced multimedia content. *Multimed. IEEE Trans.* 17, 1471–1483.
- Chen, M., Zhang, Y., Li, Y., Mao, S., Leung, V., 2015a. EMC: emotion-aware mobile cloud computing in 5G. *Netw. IEEE* 29, 32–38.
- Chen, M., Zhang, Y., Li, Y., Hassan, M., Alamri, A., 2015b. AIWAC: affective interaction through wearable computing and cloud technology. *Wirel. Commun. IEEE* 22, 20–27.
- Chen, M., Hao, Y., Li, Y., Lai, C.-F., Wu, D., 2015c. On the computation offloading at ad hoc cloudlet: architecture and service modes. *Commun. Mag., IEEE* 53, 18–24.
- Chen, X., Jiao, L., Li, W., Fu, X., 2016. Efficient multi-user computation offloading for mobile-edge cloud computing. *IEEE/ACM Trans. Netw.* 24, 2795–2808.
- Chen, M., Li, W., Li, Z., Lu, S., Chen, D., 2014. Preserving location privacy based on distributed cache pushing, in *Wireless Communications and Networking Conference (WCNC)*, 2014 IEEE, pp. 3456–3461.
- Choo, K.-K.R., 2014. Mobile cloud storage users. *IEEE Cloud Comput.*, 20–23.
- Chun, B.-G., Maniatis, P., 2009. Augmented smartphone applications Through clone cloud execution. *HotOS*, 8–11.
- Chung, K.-Y., Yoo, J., Kim, K.J., 2014. Recent trends on mobile computing and future networks. *Pers. Ubiquitous Comput.* 18, 489–491.
- De Luca, A., Von Zeuschwitz, E., Nguyen, N.D.H., Maurer, M.-E., Rubegni, E., Scipioni, M.P., et al., 2013. Back-of-device authentication on smartphones. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2389–2398.
- Dey, S., Sampalli, S., Ye, Q., 2015. A Context-Adaptive Security Framework for Mobile Cloud Computing, in *2015. In: Proceedings of the 11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pp. 89–95.
- Dhanya, N., Kousalya, G., 2015. Adaptive and Secure Application Partitioning for Offloading in Mobile Cloud Computing, *Security in Computing and Communications (ed)*. Springer, 45–53.
- Donald, A.C., Arockiam, L., 2015. A secure authentication scheme for MobiCloud, In: *Computer Communication and Informatics (ICCCI)*, 2015 International Conference on, pp. 1–6.
- Duan, Y., Zhang, M., Yin, H., Tang, Y., 2015. Privacy-preserving offloading of mobile app to the public cloud. In: *Proceedings of the 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud15)*.
- Ellouze, A., Gagnaire, M., Haddad, A., 2015. A mobile application offloading algorithm for mobile cloud computing, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2015. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 34–40.
- ElMenshawly, D., 2015. Touchscreen patterns based authentication approach for smart phones. In: *Science and Information Conference (SAI)*, pp. 1311–1315.
- Fawaz, K., Feng, H., Shin, K.G., 2015. Anatomization and Protection of Mobile Apps' Location Privacy Threats. In: *Proceedings of the 24th USENIX Security Symposium (USENIX Security 15)*, pp. 753–768.
- Feng, T., Zhao, X., Carlbunar, B., Shi, W., 2013. Continuous mobile authentication using virtual key typing biometrics, in *Trust, security and privacy in computing and communications (TrustCom)*, 2013. In: *Proceedings of the 12th IEEE international conference on*, pp. 1547–1552.
- Fernando, N., Loke, S.W., Rahayu, W., 2013. mobile cloud computing: a survey. *Future Gener. Comput. Syst.* 29, 84–106.
- Ferzli R., Khalife, I., 2011. Mobile cloud computing educational tool for image/video processing algorithms, in *Digital Signal Processing Workshop and IEEE Signal Processing Education Workshop (DSP/SPE)*, IEEE, pp. 529–533.
- Flores, H., Hui, P., Tarkoma, S., Li, Y., Srirama, S., Buyya, R., 2015. Mobile code offloading: from concept to practice and beyond. *Commun. Mag. IEEE* 53, 80–88.

- Gai, K., Qiu, M., Zhao, H., Xiong, J., 2016. Privacy-aware adaptive data encryption strategy of big data in cloud computing, in *Cyber Security and Cloud Computing (CSCloud)*, 2016 IEEE. In: *Proceedings of the 3rd International Conference on*, pp. 273–278.
- Gao, G., Zhang, W., Wen, Y., Wang, Z., Zhu, W., 2015. Towards cost-efficient video transcoding in media cloud: insights learned from user viewing patterns. *Multimed. IEEE Trans.* 17, 1286–1296.
- Giurgiu, I., Riva, O., Juric, D., Krivulev, I., Alonso, G., 2009. In: *Middleware (Ed.)*, Calling the Cloud: Enabling Mobile Phones as Interfaces to Cloud Applications 2009. Springer, 83–102.
- Guo, C., Zhuang, R., Jie, Y., Ren, Y., Wu, T., Choo, K.-K.R., 2016. Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *J. Med. Syst.* 40, 235.
- Han, Y., Chan, J., Alpcan, T., Leckie, C., 2015. Using virtual machine allocation policies to defend against co-resident attacks in cloud computing. *IEEE Trans. Dependable Secur. Comput.*
- Hao, Z., Tang, Y., Zhang, Y., Novak, E., Carter, N., Li, Q., 2015. SMOC: A secure mobile cloud computing platform. In: *Computer Communications (INFOCOM)*, 2015 IEEE Conference on, pp. 2668–2676.
- Harrow, S., Gupta, S., Sardana, A., Abraham, A., 2012. Secure private cloud architecture for mobile infrastructure as a service. In: *Services (SERVICES)*, 2012 IEEE Eighth World Congress on, pp. 149–154.
- Hossain, E., Hasan, M., 2015. 5G cellular: key enabling technologies and research challenges. *Instrum. Meas. Mag. IEEE* 18, 11–21.
- Huerta-Canepa, G., Lee, D., 2010. A virtual cloud computing provider for mobile devices. In: *Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, p. 6.
- Hurel, G., Badonnel, R., Lahmadi, A., Festor, O., 2015. Towards Cloud-Based Compositions of Security Functions For Mobile Devices. In: *IFIP/IEEE International Symposium on Integrated Network Management (IM'15)*, p. 6.
- Imgraben, J., Engelbrecht, A., Choo, K.-K.R., 2014. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behav. Inf. Technol.* 33, 1347–1360.
- Iqbal, S., Kiah, M.L.M., Dhaghghi, B., Hussain, M., Khan, S., Khan, M.K., et al., 2016. On cloud security attacks: a taxonomy and intrusion detection and prevention as a service. *J. Netw. Comput. Appl.* 74, 98–120.
- Jarabek, C., Barrera, R., Aycock, J., 2012. Thinav: Truly lightweight mobile cloud-based anti-malware. In: *Proceedings of the 28th Annual Computer Security Applications Conference*, pp. 209–218.
- Jeong, Y.S., Park, J.S., Park, J.H., 2013. An efficient authentication system of smart device using multi factors in mobile cloud service architecture. *Int. J. Commun. Syst.*
- Jin, S., Ahn, J., Seol, J., Cha, S., Huh, J., Maeng, S., 2015. H-SVM: hardware-assisted secure virtual machines under a vulnerable hypervisor. *Comput. IEEE Trans.* 64, 2833–2846.
- Jin, Y., Tian, C., He, H., Wang, F., 2015. A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing, in *Big Data and Cloud Computing (BDCloud)*, 2015 IEEE. In: *Proceedings of the Fifth International Conference on*, pp. 172–179.
- Juliadotter, N.V., Choo, K.-K.R., 2015. Cloud attack and risk assessment taxonomy. *IEEE Cloud Comput.* 2, 14–20.
- Khalil, I., Khreishah, A., Azeem, M., 2014. Consolidated Identity Management System for secure mobile cloud computing. *Comput. Netw.* 65, 99–110.
- Khan, A.N., Kiah, M.M., Khan, S.U., Madani, S.A., 2013a. Towards secure mobile cloud computing: a survey. *Future Gener. Comput. Syst.* 29, 1278–1299.
- Khan, A.N., Kiah, M.M., Madani, S.A., Ali, M., 2013b. Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. *J. Supercomput.* 66, 1687–1706.
- Khan, A.N., Kiah, M.M., Ali, M., Madani, S.A., Shamshirband, S., 2014. BSS: block-based sharing scheme for secure data storage services in mobile cloud environment. *J. Supercomput.* 70, 946–976.
- Khan, A.N., Kiah, M.M., Ali, M., Shamshirband, S., 2015. A cloud-Manager-based Re-Encryption scheme for mobile users in cloud environment: a hybrid approach. *J. Grid Comput.* 13, 651–675.
- Kovachev, D., Renzel, D., Klamma, R., Cao, Y., 2010. Mobile community cloud computing: emerges and evolves, in *Mobile Data Management (MDM)*, 2010. In: *Proceedings of the Eleventh International Conference on*, pp. 393–395.
- Kumari, S., Li, X., Wu, F., Das, A.K., Choo, K.-K.R., Shen, J., 2017. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Gener. Comput. Syst.* 68, 320–330.
- Lei, L., Sengupta, S., Pattanaik, T., Gao, J., 2015. McloudDB: A Mobile Cloud Database Service Framework, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2015. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 6–15.
- Li, H., Liu, D., Dai, Y., Luan, T.H., Shen, X., 2015. Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage. *Emerg. Top. Comput. IEEE Trans.* 3, 127–138.
- Li, J., Li, J., Chen, X., Liu, Z., Jia, C., 2014. Privacy-preserving data utilization in hybrid clouds. *Future Gener. Comput. Syst.* 30, 98–106.
- Li, Y., Gai, K., Ming, Z., Zhao, H., Qiu, M., 2016. Interconnected access controls for secure financial services on multimedia big data in cloud systems. *ACM Trans. Multimed. Comput. Commun. Appl. (TOMM)* 12, 67.
- Liang, H., Han, C., Zhang, D., Wu, D., 2014. A Lightweight Security Isolation Approach for Virtual Machines Deployment. In: *Information Security and Cryptology*, pp. 516–529.
- Liu, D., Dai, Y., Luan, T., Yu, S., 2015. Personalized search over encrypted data with efficient and secure updates in mobile clouds. *IEEE Trans. Emerg. Top. Comput.*
- Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., et al., 2013. Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. *Wirel. Commun. IEEE* 20, 14–22.
- Liu, J.K., Au, M.H., Susilo, W., Liang, K., Lu, R., Srinivasan, B., 2015. Secure sharing and searching for real-time video data in mobile cloud. *Netw. IEEE* 29, 46–50.
- Liu, L., Zhang, X., Yan, G., Chen, S., 2009. Exploitation and threat analysis of open mobile devices, In: *Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, pp. 20–29.
- Louk, M., Lim, H., 2015. Homomorphic encryption in mobile multi cloud computing, in *Information Networking (ICOIN)*, 2015 International Conference on, pp. 493–497.
- Luan, T.H., Gao, L., Li, Z., Xiang, Y., Sun, L., 2015. Fog Computing: Focusing on Mobile Users at the Edge, *arXiv preprint arXiv:1502.01815*.
- Mao, Y., You, C., Zhang, J., Huang, K., Letaief, K.B., 2017. Mobile edge computing: survey and Research outlook. *arXiv Prepr arXiv* 1701, 01090.
- Meilander, D., Glinka, F., Gorchach, S., Lin, L., Zhang, W., Liao, X., 2014. Bringing mobile online games to clouds, in *Computer Communications Workshops (INFOCOM WKSHPS)*, 2014. IEEE Conference on, pp. 340–345.
- Meilander, D., Glinka, F., Gorchach, S., Lin, L., Zhang, W., Liao, X., 2014. Using mobile cloud computing for real-time online applications, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2014. In: *Proceedings of the 2nd IEEE International Conference on*, pp. 48–56.
- Meng, T., Wang, Q., Wolter, K., 2015. Model-Based Quantitative Security Analysis of Mobile Offloading Systems under Timing Attacks, *Analytical and Stochastic Modelling Techniques and Applications (ed)*. Springer, 143–157.
- Milligan, P.M., Hutcheson, D., 2008. Business risks and security assessment for mobile devices. *Inf. Syst. Control J.* 1, 24.
- Mohammad, A.-R., Elham, A.-S., Jararweh, Y., 2015. AMCC: Ad-hoc based mobile cloud computing modeling. *Procedia Comput. Sci.* 56, 580–585.
- Mollah, M.B., Azad, M.A.K., Vasilakos, A., 2017. Secure data sharing and Searching at the edge of cloud-assisted Internet of Things. *IEEE Cloud Comput.* 4, 34–42.
- Mollah, M.B., Islam, K.R., Islam, S.S., 2012. Next generation of computing through cloud computing technology, in *Electrical & Computer Engineering (CCECE)*, 2012 In: *Proceedings of the 25th IEEE Canadian Conference on*, pp. 1–6.
- Nan, G., Mao, Z., Li, M., Zhang, Y., Gjessing, S., Wang, H., et al., 2014. Distributed resource allocation in cloud-based wireless multimedia social networks. *Netw., IEEE* 28, 74–80.
- Niu, B., Li, Q., Zhu, X., Cao, G., Li, H., 2015. Enhancing privacy through caching in location-based services. In: *Computer Communications (INFOCOM)*, 2015 IEEE Conference on, pp. 1017–1025.
- Odelu, V., Das, A.K., Rao, Y.S., Kumari, S., Khan, M.K., Choo, K.-K.R., 2016. Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. *Comput. Stand. Interfaces.*
- Olafare, O., Parhizkar, H., Vem, S., 2015. A New Secure Mobile Cloud Architecture," *arXiv preprint arXiv:1504.07563*.
- Online: 2016] A Report of Worldwide Smartphone Markets: 2011 to 2015, May 2011: (http://www.researchandmarkets.com/research/7a1189/worldwide_smartphone).
- Online: 2016] ABI Research Report on Mobile Cloud Computing; (<https://www.abiresearch.com/research/product/1005283-mobile-cloud-applications/>).
- Online: 2016] Device Policy for Android: Overview for Users: (<http://www.google.com/support/mobile/bin/answer.py?hl=en&answer=190930>).
- Online: 2016] Mobile Cloud Computing Forum; (<http://www.mobilecloudcomputingforum.com>).
- Online: 2016] Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications: (<https://www.itu.int/itudoc/itu-t/85097.pdf>).
- Online: 2016] US National Security Agency: Information Assurance: (http://www.nsa.gov/ia/ia_at_nsa/index.shtml).
- Osanaieye, O., Choo, K.-K.R., Dlodlo, M., 2016. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *J. Netw. Comput. Appl.* 67, 147–165.
- Owens, R., Wang, W., 2013. Preserving Data Query Privacy in Mobile Mashups through Mobile Cloud Computing, in *Computer Communications and Networks (ICCCN)*, 2013. In: *Proceedings of the 22nd International Conference on*, pp. 1–5.
- Paladi, N., Gehrmann, C., Michalas, A., 2016. Providing user security guarantees in public infrastructure clouds. *IEEE Trans. Cloud Comput.*
- Park, I.-S., Lee, Y.-D., Jeong, J., 2013. Improved Identity Management Protocol for Secure Mobile Cloud Computing, in *System Sciences (HICSS)*, 2013. In: *Proceedings of the 46th Hawaii International Conference on*, pp. 4958–4965.
- 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. *J. Netw. Comput. Appl.* 64, 12–22.
- Patel, P., Patel, R., 2015. Security in CloneCloud for Mobile Cloud Computing, in *Communication Systems and Network Technologies (CSNT)*, 2015. In: *Proceedings of the Fifth International Conference on*, pp. 752–756.
- Peng, J., Choo, K.-K.R., Ashman, H., 2016. User profiling in intrusion detection: a review. *J. Netw. Comput. Appl.* 72, 14–27.
- Pokharel, S., Choo, K.-K.R., Liu, J., 2017. Mobile cloud security: an adversary model for lightweight browser security. *Comput. Stand. Interfaces* 49, 71–78.
- Popa, D., Cremene, M., Borda, M., Boudaoud, K., 2013. A security framework for mobile cloud applications. In: *Roedunet International Conference (RoEduNet)*, 2013 11th, pp. 1–4.
- Prokhorenko, V., Choo, K.-K.R., Ashman, H., 2016. Web application protection techniques: a taxonomy. *J. Netw. Comput. Appl.* 60, 95–112.
- Psannis, K., Xinogalos, S., Sifaleras, A., 2014. Convergence of Internet of things and mobile cloud computing. *Syst. Sci. Control Eng.: Open Access J.* 2, 476–483.
- Qiu, M., Gai, K., Thuraishingham, B., Tao, L., Zhao, H., 2016. Proactive user-centric secure

- data scheme using attribute-based semantic access controls for mobile clouds in financial industry. *Future Gener. Comput. Syst.*
- Quick, D., Choo, K.-K.R., 2016. Pervasive social networking forensics: intelligence and evidence from mobile device extracts. *J. Netw. Comput. Appl.*
- Racic, R., Ma, D., Chen, H., 2006. Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery. In: *Securecomm and Workshops*, pp. 1–10.
- Raj, M., Di Francesco, M., Das, S.K., 2012. Secure mobile cloud computing. *Handb. Secur. Cyber-Phys. Crit. Infrastruct.*, 411–429.
- Rappaport, T.S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., et al., 2013. Millimeter wave mobile communications for 5G cellular: it will work!. *Access, IEEE* 1, 335–349.
- Rassan, I.A., AlShaher, H., 2014. Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA). In: *2014 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 157–161.
- S. Dey, S. Sampalli, and Q. Ye, "A light-weight authentication scheme based on message digest and location for mobile cloud computing," in *Performance Computing and Communications Conference (IPCCC)*, 2014 IEEE International, 2014, pp. 1–2.
- Saab, S.A., Saab, F., Kayssi, A., Chehab, A., Elhajj, I.H., 2015. Partial mobile application offloading to the cloud for energy-efficiency with security measures. *Sustain. Comput.: Inform. Syst.* 8, 38–46.
- Sanaei, Z., Abolfazli, S., Gani, A., Shiraz, M., 2012. SAMI: service-based arbitrated multi-tier infrastructure for mobile cloud computing, in *Communications in China Workshops (ICCC)*, 2012. In: *Proceedings of the 1st IEEE International Conference on*, pp. 14–19.
- Satyanarayanan, M., Bahl, P., Caceres, R., Davies, N., 2009. The case for vm-based cloudlets in mobile computing. *Pervasive Comput. IEEE* 8, 14–23.
- Sgandurra, D., Lupu, E., 2016. Evolution of attacks, threat models, and solutions for virtualized systems. *ACM Comput. Surv. (CSUR)* 48, 46.
- Sharma, R., Kumar, S., Trivedi, M.C., 2013. Mobile cloud computing: A needed shift from cloud to mobile cloud, in *Computational Intelligence and Communication Networks (CICN)*, 2013. In: *Proceedings of the 5th International Conference on*, pp. 536–539.
- Sharma, R., Kumar, S., Trivedi, M.C., 2013. Mobile Cloud Computing: Bridging the Gap between Cloud and Mobile Devices," in *Computational Intelligence and Communication Networks (CICN)*, 2013 In: *Proceedings of the 5th International Conference on*, pp. 553–555.
- Shi, Y., Abhilash, S., Hwang, K., 2015. Cloudlet mesh for securing mobile clouds from intrusions and network attacks, in *Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2015. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 109–118.
- Shon, T., Cho, J., Han, K., Choi, H., 2014. Toward advanced mobile cloud computing for the Internet of Things: Current issues and future direction. *Mob. Netw. Appl.* 19, 404–413.
- Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., et al., 2016. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Trans. Inf. Forensics Secur.* 11, 877–892.
- Sookhak, M., Gani, A., Khan, M.K., Buyya, R., 2017. Dynamic remote data auditing for securing big data storage in cloud computing. *Inf. Sci.* 380, 101–116.
- Suarez-Tangil, G., Tapiador, J.E., Peris-Lopez, P., Ribagorda, A., 2014. Evolution, detection and analysis of malware for smart devices. *Commun. Surv. Tutor. IEEE* 16, 961–987.
- Suo, H., Liu, Z., Wan, J., Zhou, K., 2013. Security and privacy in mobile cloud computing, in *Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013. 9th International, pp. 655–659.
- Sweeney, L., 2002. k-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* 10, 557–570.
- Tan, J., Gandhi, R., Narasimhan, P., 2014. STOVE: Strict, Observable, Verifiable Data and Execution Models for Untrusted Applications, in *Cloud Computing Technology and Science (CloudCom)*, 2014 IEEE. In: *Proceedings of the 6th International Conference on*, pp. 644–649.
- Teing, Y.Y., Dehghantanha, A., Choo, K.K.R., Dargahi, T., Conti, M., 2016. Forensic investigation of cooperative storage cloud service: symform as a case study. *J. Forensic Sci.*
- Tep, K.S., Martini, B., Hunt, R., Choo, K.-K.R., 2015. A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management, in *Trustcom/BigDataSE/ISPA*, 2015 IEEE, pp. 1073–1080.
- Tang, L., Ouyang, L., Tsai, W.-T., 2015. Multi-factor web API security for securing Mobile Cloud. In: *Fuzzy Systems and Knowledge Discovery (FSKD)*, 2015 12th International Conference on, pp. 2163–2168.
- Tian, H., Chen, Y., Chang, C.-C., Jiang, H., Huang, Y., Chen, Y., et al., 2015. Dynamic-hash-table based public auditing for secure cloud storage. *IEEE Trans. Serv. Comput.*
- Tsai, J.-L., Lo, N.-W., 2015. A Privacy-Aware authentication scheme for Distributed mobile cloud computing services. *IEEE Syst. J.* 9, 805–815, (21 May).
- Tysowski, P., Hasan, M.A., 2011. Towards secure communication for highly scalable mobile applications in cloud computing systems. *Cent. Appl. Cryptogr. Res. Univ. Waterloo Tech. Rep. CACR* 33, 2011.
- Tysowski, P.K., Hasan, M.A., 2013. Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds. *Cloud Comput. IEEE Trans.* 1, 172–186.
- Vaezpour, S.Y., Zhang, R., Wu, K., Wang, J., Shojia, G.C., 2016. A new approach to mitigating security risks of phone clone Co-location Over mobile clouds. *J. Netw. Comput. Appl.*
- Vaquero, L.M., Roderio-Merino, L., 2014. Finding your way in the fog: towards a comprehensive definition of fog computing. *ACM SIGCOMM Comput. Commun. Rev.* 44, 27–32.
- Walls, J., Choo, K.-K. R., 2015. A Review of Free Cloud-Based Anti-Malware Apps for Android, In: *Trustcom/BigDataSE/ISPA*, 2015 IEEE, pp. 1053–1058.
- Wang, H., Wu, S., Chen, M., Wang, W., 2014. Security protection between users and the mobile media cloud. *Commun. Mag., IEEE* 52, 73–79.
- Wang, S., Tu, G.-H., Ganti, R., He, T., Leung, K., Tripp, H., et al., 2013. Mobile micro-cloud: Application classification, mapping, and deployment. In: *Proceedings Annual Fall Meeting of ITA (AMITA)*.
- Wen, Y., Zhu, X., Rodrigues, J.J., Chen, C.W., 2014. Cloud mobile media: reflections and outlook. *Multimed. IEEE Trans.* 16, 885–902.
- Wu, D., Wang, J., Cai, Y., Guizani, M., 2015. Millimeter-wave multimedia communications: challenges, methodology, and applications. *Commun. Mag. IEEE* 53, 232–238.
- Xia, Y., Liu, Y., Tan, C., Ma, M., Guan, H., Zang, B., et al., 2015. TinMan: eliminating confidential mobile data exposure with security oriented offloading. In: *Proceedings of the Tenth European Conference on Computer Systems*, p. 27.
- Xiu-feng, Q., Jian-Wei, L., Peng-Chuan, Z., 2011. Secure cloud computing architecture on mobile internet, in *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, 2011. In: *Proceedings of the 2nd International Conference on*, pp. 619–622.
- Yang, Y., Zhu, H., Lu, H., Weng, J., Zhang, Y., Choo, K.-K.R., 2016. Cloud based data sharing with fine-grained proxy re-encryption. *Pervasive Mob. Comput.* 28, 122–134.
- Yang, X., Pan, T., Shen, J., 2010. On 3G mobile e-commerce platform based on cloud computing, in *Ubi-media Computing (U-Media)*, 2010. In: *Proceedings of the 3rd IEEE International Conference on*, pp. 198–201.
- Yang, Y., Liu, J.K., Liang, K., Choo, K.-K.R., Zhou, J., 2015. Extended proxy-assisted approach: achieving revocable fine-grained encryption of cloud data, in *European Symposium on Research in Computer Security*, pp. 146–166.
- Yin, Z., Yu, F.R., Bu, S., Han, Z., 2015. Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud. *Wirel. Commun. IEEE Trans.* 14, 4020–4033.
- Yu, Y., Mu, Y., Ni, J., Deng, J., Huang, K., 2014. Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage, Network and System Security ed.. Springer, 28–40.
- Yu, Y., Li, Y., Au, M.H., Susilo, W., Choo, K.-K.R., Zhang, X., 2016. Public cloud data auditing with practical key update and zero knowledge privacy. In: *Australasian Conference on Information Security and Privacy*, pp. 389–405.
- Zhang, H., Yu, N., Wen, Y., 2015. Mobile cloud computing based privacy protection in location-based information survey applications. *Secur. Commun. Netw.* 8, 1006–1025.
- Zhang, J., Zhao, X., 2015. Efficient chameleon hashing-based privacy-preserving auditing in cloud storage. *Clust. Comput.*, 1–10.
- Zhang, Y., Su, S., Wang, Y., Chen, W., Yang, F., 2014. Privacy-assured substructure similarity query over encrypted graph-structured data in cloud. *Secur. Commun. Netw.* 7, 1933–1944.
- Zhang, Y., Zheng, D., Chen, X., Li, J., Li, H., 2016. Efficient attribute-based data sharing in mobile clouds. *Pervasive Mob. Comput.* 28, 135–149.
- Zhang, X., Schiffman, J., Gibbs, S., Kunjithapatham, A., Jeong, S., 2009. Securing elastic applications on mobile devices for cloud computing. In: *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 127–134.
- Zhao, X., Feng, T., Shi, W., 2013. Continuous mobile authentication using a novel graphic touch gesture feature, in *Biometrics: Theory, Applications and Systems (BTAS)*, 2013 IEEE. In: *Proceedings of the Sixth International Conference on*, pp. 1–6.
- Zhong, H., Xiao, J., 2014. Design for a cloud-based hybrid Android application security assessment framework. In: *Reliability, Maintainability and Safety (ICRMS)*, 2014 International Conference on, pp. 539–546.
- Zhong, L., Wang, B., Wei, H., 2012. Cloud computing applied in the mobile internet, in *Computer Science & Education (ICCSE)*, 2012. In: *Proceedings of the 7th International Conference on*, pp. 218–221.
- Zhu, W., Luo, C., Wang, J., Li, S., 2011. Multimedia cloud computing. *Signal Process. Mag. IEEE* 28, 59–69.
- Zonouz, S., Houmansadr, A., Berthier, R., Borisov, N., Sanders, W., 2013. Secloud: a cloud-based comprehensive and lightweight security solution for smartphones. *Comput. Secur.* 37, 215–227.